Czas informacji
Prawo nowych technologii • Informacja w administracji i gospodarce
ISSN 2081-6189 kwartalnik 2(7)/2011

Prawo do bycia zapomnianym

Bezpieczeństwo procesu publikacji ustaw i rozporządzeń
Michał Tabor, Przemysław Momot

Powszechny dostęp do orzeczeń sądowych
Kazimierz Chojna

E-dowód osobisty - projekt zmian w ustawie o dowodzie osobistym
Mirosław Kutyłowski

Co dalej z ICT w nowej perspektywie finansowej UE?
Dariusz Bogucki

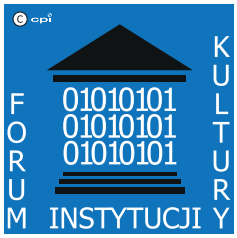
Upgrade oprogramowania jako przedmiot zamówienia publicznego
Wojciech Kaliński

Problemy w projektach informatycznych realizowanych na potrzeby administracji publicznej
Izabela Adamska

Bohater naszych czasów
Edwin Bendyk

cpi
centrum promocji informatyki
www.cpi.com.pl

centrum promocji informatyki
www.cpi.com.pl



FORUM INSTYTUCJI KULTURY
PROBLEMY CYFRYZACJI ZASOBÓW MUZEÓW, BIBLIOTEK I ARCHIWÓW

19 października 2011 r., Centrum Nauki Kopernik, Warszawa

RADA PROGRMOWA:
dr Edwin Bendyk, prof. dr hab. inż. Wojciech Cellary,
prof. dr hab. Dorota Folga-Januszewska, dr Henryk Hollender,
dr Tomasz Makowski, prof. dr hab. Ewa Nowińska, dr Wojciech R. Wiewiórowski

Sesja inauguracyjna:
Cyfryzacja zasobów a elektroniczna gospodarka oparta na wiedzy
dr Edwin Bendyk, prof. dr hab. Wojciech Cellary
Standardy procesu digitalizacji
dr Grzegorz Płoszajski, Politechnika Warszawska,
Biblioteka Główna Instytutu Automatyki i Informatyki Stosowanej
Cyfrowe biblioteki i archiwa - w świetle polskiego i europejskiego prawa autorskiego
dr Sybilla Stanisławska-Kloc, Uniwersytet Jagielloński
Cyfryzacja dzieł kultury - konsekwencje cywilizacyjne - przemiany mentalne i społeczne (psychologiczne aspekty cyfryzacji)
prof.. dr hab. Dorota Folga-Januszewska, prof. dr hab. Ryszard W. Kluszczyński,
prof.. dr hab. Kazimierz Krzysztofek
Udostępnianie zasobów dziedzictwa narodowego przez Internet. Ochrona danych w zbiorach cyfrowych
dr Wojciech R. Wiewiórowski, Generalny Inspektor Ochrony Danych Osobowych

Trzy równoległe sesje tematyczne:
Wirtualne Muzea, moderator sesji: prof. dr hab. Dorota Folga-Januszewska
Cyfrowe Biblioteki, moderator sesji: dr Henryk Hollender
Elektroniczne Archiwa, moderator sesji: dr Sylwia Kotecka

www.cpi.com.pl/imprezy/2011/fik

Biuro organizacyjne:
Centrum Promocji Informatyki sp. z o.o.
ul. Międzyborska 50, 04-041 Warszawa
tel.: 22 870 69 78, faks: 22 870 69 95
email: cpi@cpi.com.pl

NAUKA

4 **Co dalej z ICT w nowej perspektywie finansowej UE?**
Dariusz Bogucki

10 **E-dowód osobisty - projekt zmian w ustawie o dowodzie osobistym**
Mirosław Kutyłowski

17 **Prawo do bycia zapomnianym**
Arwid Mednis

25 **Podpis elektroniczny – prawo i rzeczywistość**
Robert Poznański, Daniel Wachnik

31 **Przetwarzanie przez organizację pożytku publicznego danych osobowych osób, które przekazały za pośrednictwem organów skarbowych 1% podatku**
Jan Byrski

37 **Upgrade oprogramowania jako przedmiot zamówienia publicznego. Rozważania na tle zamówień na systemy informacji prawnej**
Wojciech Kaliński

49 **Biuletyny Informacji Publicznej sądów i prokuratur w województwie śląskim – raport z badania**
Grzegorz Wójkowski

PUBLICYSTYKA

54 **Bezpieczeństwo procesu publikacji ustaw i rozporządzeń**
Przemysław Momot, Michał Tabor

59 **Powszechny dostęp do orzeczeń sądowych**
Kazimierz Chojna

63 **Nowe zasady prowadzenia ewidencji ludności**
Katarzyna Czajkowska-Matosiuk

70 **Zmiany w postępowaniu administracyjnym w 2011 roku**
Anita Jackiewicz

74 **Są nowe akty wykonawcze do informatyzacji, czyli ePUAP-ką po łapkach**
Sebastian Paweł Zalipski

80 **Jaka będzie przyszłość elektronicznej administracji? Część II - perspektywy**
Dariusz Bogucki

86 **Czy Europa potrzebuje strategii cyfrowej?**
Edyta Marcinkowska

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

STAŁE RUBRYKI

93 **Ochrona danych osobowych: Ochrona danych osobowych a zasada otwartości w prawie Unii Europejskiej**
Piotr Drobek

97 **Zarządzanie projektami: Dobre praktyki w zarządzaniu projektami**
Ewa Szczepańska

104 **Zarządzanie projektami: Problemy w projektach informatycznych realizowanych na potrzeby administracji publicznej**
Izabela Adamska

110 **Przegląd orzecznictwa w zakresie zamówień publicznych: Wyrok Krajowej Izby Odwoławczej z dnia 20 lipca 2010 r., sygn. akt: KIO 1408/10**
Wojciech Kaliński

113 **Zakończyła się XVI edycja Forum Informatyki w Administracji**

116 **Bohater naszych czasów**
Edwin Bendyk

118 **Bibliografia zagadnień prawno-informatycznych 2010**
Wojciech R. Wiewiórowski

W kolejnym numerze:

W najbliższym numerze m.in.:

- Zasada uczciwej konkurencji i równego traktowania wykonawców w zamówieniach publicznych IT – teoria i praktyka - Tomasz Filipowicz, Agnieszka Leszczyńska
- Do złożenia skargi podpis elektroniczny nie jest wymagany - Jacek Murzydło
- Wykluczenie cyfrowe w Polsce - Edyta Marcinkowska
- Zarządzanie ryzykiem w projektach - Ewa Szczepańska
- VAT w wersji elektronicznej - Katarzyna Czajkowska-Matosiuk
- Wolne i otwarte oprogramowanie a Software-as-a-Service - Bohdan Widła
- Podpisy grupowe i ich zastosowanie - Przemysław Kubiak
- Zarządzanie projektami IT w administracji publicznej - Izabela Adamska, Marcin Kędzierski
- Jaka będzie przyszłość elektronicznej administracji? Część III - nowe idee - Dariusz Bogucki

Wiesław Paluszyński redaktor naczelny
wieslaw.paluszynski@czasinformacji.pl

Także w informatyce rządowej zaczynamy mieć „chiński syndrom". Co prawda, nie dotyczy on chińczyków i budowy autostrady, ale istota problemu jest podobna. Mieliśmy dostać nowoczesny Dowód Osobisty, będący kluczem do systemów teleinformatycznych administracji publicznej i przy okazji kartą zdrowotną. Wszystkie systemy realizowane w Polsce miały uwzględnić fakt istnienia tego „klucza" od 1 lipca 2011 roku. Kto uwierzył i tak zrobił, został właśnie postawiony w sytuacji bez wyjścia. Nie dość, że w związku z decyzją MSWiA nowy Dowód Osobisty będzie dopiero od 1 lipca 2013 roku, to także jego funkcje będą nieco inne. Aby wiedzieć, co naprawdę zrobiono w tej niekonsultowanej ani z organizacjami zawodowymi informatyków, ani z Izbami Gospodarczymi, ani także Komisją Wspólna Rządu i Samorządu nowelizacji, należy przeczytać w tym numerze artykuł prof. Mirosława Kutyłowskiego. Swoją drogą, jest coraz ciekawiej, bo profesor został właśnie zaproszony jako oficjalny konsultant rządu niemieckiego w uznaniu jego opracowań dotyczących części elektronicznej dokumentów identyfikacyjnych, a nasze rodzime władze nie widzą potrzeby z jego wiedzy korzystać. Cóż, jak widać po publikacjach dostępnych w Internecie, mamy całe rzesze ekspertów mających publikowany dorobek w tym zakresie…

Tym, co uwierzyli w Dowód Osobisty, pozostaje więc szybko skorzystać z funkcji ePUAP i zaufanego profilu, który po prawie dwóch latach zapowiedzi, zgodnie z prasowymi informacjami, pojawił się jako dostępna usługa dla obywateli. Nikt się nie zająknął, dlaczego to trwało dodatkowe półtora roku od pierwszej zapowiedzi, że za chwilę będzie, ale nie bądźmy małostkowi. Chciałem, pisząc ten wstępniak, skorzystać z własnych doświadczeń ePUPA (oj przepraszam, to samoistna poprawka edytora) - ePUAP, ale niestety, „chwilowo zniknął z sieci". Pozostaje więc skierować Szanownych Czytelników do artykułu Sebastiana Pawła Zalipskiego i jego doświadczeń z tą platformą.

Dla chcących zrozumieć, dlaczego tak jest z projektami, polecam artykuł Izabeli Adamskiej o problemach w projektach w administracji publicznej. Warto przy tej okazji sięgnąć kilka numerów wstecz do artykułu Michała Tabora o problemach z interoperacyjnością tych projektów. Wnikliwym polecam wejście na stronę http://www.wwpe.gov.pl/index.php?params[section_id]=20&params[category_id]=331 i przejrzenie umieszczonych tam analiz kompatybilności dla projektów realizowanych w ramach 7 osi. Po przeczytaniu tych dokumentów i przejrzeniu opublikowanej tam „mapy kompatybilności" nasunął mi się nieodparty wniosek, że odkryliśmy, jak zamiast uzyskania interoperacyjności systemów w administracji publicznej zrobić „e-węzeł gordyjski". Czytając, iż w ramach Polskiej Prezydencji w UE będziemy w Poznaniu gospodarzem konferencji dotyczącej e-administracji w UE, mam nadzieję, że nie będziemy jednak chwalić się publicznie na europejskim forum, jak taki „e-węzeł" zrobić.

Mamy bowiem naprawdę parę ciekawych doświadczeń. W tym numerze polecam artykuł Michała Tabora o bezpieczeństwie publikowanych w Internecie aktów prawnych, publikację Dariusza Boguckiego o nowej strategii UE w zakresie informatyzacji, a także dokończenie artykułu o e-government. O powszechnym dostępie do orzeczeń sądów administracyjnych pisze Kazimierz Chojna. A poza tym tradycyjnie - trochę prawa, o zmianach w KPA, zamówieniach publicznych, danych osobowych, trochę technologii podpisu elektronicznego.

W kolejnym numerze spróbujemy wrócić do służby zdrowia, a także do tematów podejmowanych w trakcie majowo-czerwcowych rozmów premiera z internautami, po wakacjach nam się przyda.

Miłej lektury na progu urlopu

Co dalej z ICT w nowej perspektywie finansowej UE?

Dariusz Bogucki

Wszystko wskazuje na to, że wraz z początkiem polskiej Prezydencji Komisja Europejska ogłosi, jak widzi nowy okres programowania finansowego, czyli wieloletni plan budżetu wspólnoty na lata 2014-2020. Warto zatem przyjrzeć się bliżej temu tematowi nie tylko dlatego, że będzie to jeden z głównych tematów naszej Prezydencji. Ostatnio zapanowało (zwłaszcza w sektorze publicznym) dziwne przekonanie, że w nowym okresie programowania nie zmienią się zasady, wedle których finansujemy przedsięwzięcia związane z ICT z tzw. funduszy strukturalnych UE. Opublikowane robocze dokumenty Komisji wskazują, że czekają nas znaczące zmiany w tym obszarze.

Wyzwania dla regionów w horyzoncie roku 2020

Zanim omówimy szczegółowo propozycje zmian budżetowych, jakie zaproponowała Komisja Europejska, należy przypomnieć, że stanowią one wynik wieloletniej refleksji Komisji nad dotychczasowymi rezultatami polityki strukturalnej.

Szczególną rolę w konstruowaniu założeń polityki strukturalnej na lata 2014-2020 odegrały dwa opracowania: opublikowany jeszcze w 2008 roku Raport *„Regiony 2020*" oraz *„Czynnik regionalny w procesie zmian technologicznych w horyzoncie 2020 r."* opracowany jesienią 2010 roku.

W pierwszym z nich przedstawiono wstępną analizę prawdopodobnego wpływu na regiony czterech największych wyzwań cywilizacyjnych, z którymi zmaga się Europa: globalizacji, tendencji demograficznych, zmian klimatu oraz zużycia energii i jej dostaw.

Raport ten wskazuje, że regiony o konkurencyjnej i innowacyjnej gospodarce skorzystają na procesie globalizacji, natomiast regiony słabo wpisujące się w tematykę gospodarki opartej na wiedzy (w tym regiony na południu i wschodzie UE) znajdą się w niekorzystnej pozycji. Jednakże w sprawozdaniu wskazano na to, że te regiony, w których znajdują się duże ośrodki miejskie, przyciągające najlepiej wykształconych mieszkańców i najnowocześniejsze sektory przemysłu, będą się rozwijać dynamicznie.

Do 2020 r. spadnie liczba ludności w ok. jednej trzeciej regionów europejskich. Większość tych regionów położona jest w nowych państwach członkowskich Europy Środkowej i Wschodniej, we wschodnich Niemczech, południowych Włoszech i północno-zachodniej Hiszpanii. W sprawozdaniu przewiduje się, że zmiany klimatu wywrą, w mniejszym lub większym stopniu, negatywny wpływ na większość regionów Europy. Raport wskazuje szczegółowo, że skutki tych zmian będą odczuwalne w większości sektorów gospodarki, także tych najbardziej innowacyjnych, a nie tylko w turystyce, produkcji energii, rolnictwie i rybołówstwie.

Drugi z raportów skupił się na badaniu korelacji pomiędzy politykami regionalnymi a rozwojem gospodarki opartej na wiedzy.

Raport wskazał na przyczyny dysproporcji między poszczególnymi państwami członkowskimi i regionami UE w dziedzinie

innowacji i działalności badawczo-rozwojowej oraz utrzymującą się przepaść w porównaniu z najważniejszymi konkurentami Unii na arenie światowej. Raport wskazał na konieczność budowy w regionach strategicznych partnerstwa między podmiotami z sektorów przemysłu, badań naukowych, edukacji oraz sektora publicznego w obszarze przejścia. Takie partnerstwa szczególnie skutecznie funkcjonują w tzw. regionach high-tech: 17 regionach w Niemczech, Finlandii, Szwecji i Holandii, w których ulokowane są firmy z obszaru nowych technologii ze szczególnym podkreśleniem ICT. Są to regiony o ponadprzeciętnej zdolności absorpcji, zdolności tworzenia i zapewnienia dostępu do wiedzy. Regiony te wykazują ponadprzeciętny poziom rozwoju gospodarczego i szybki wzrost, aczkolwiek tylko w obszarach nowych technologii.

Wspólnym elementem obydwu raportów było wskazanie na technologie informacyjne i komunikacyjne jako główny motor, dzięki któremu Europa stanie się bardziej innowacyjna, szybciej reagująca na zmieniające się warunki rynkowe i preferencje konsumentów oraz kształtująca społeczeństwo i gospodarkę przyjazną dla innowacji.

Wnioski te stanowiły fundament proponowanych zmian europejskiej polityki spójności.

Nowe ramy finansowania w duchu strategii „Europa 2020"

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.

Działania Komisji pokazują, jak wielką rolę przywiązuje ona do strategii „Europa 2020" i jej inicjatyw przewodnich. W ubiegłorocznym przeglądzie budżetu UE Komisja przedstawiła zarys nowej strategii programowania polityki spójności. Jej kluczowym elementem miałaby być ścisła integracja wszystkich polityk UE (w tym polityki regionalnej, która jest bazą działania tzw. funduszy strukturalnych) ze strategią „Europa2020" i jej siedmioma kluczowymi inicjatywami.

Nowa strategia programowania miałaby obejmować:

- **wspólne ramy strategiczne (WRS)** przyjęte przez Komisję, które przekładałyby założenia i cele strategii „Europa 2020" na priorytety w zakresie inwestycji. Ramy objęłyby Fundusz Spójności, Europejski Fundusz Rozwoju Regionalnego, Europejski Fundusz Społeczny, ale też Europejski Fundusz Rolny na rzecz Rozwoju Obszarów Wiejskich i Europejski Fundusz Rybacki.
- **umowę o partnerstwie w dziedzinie rozwoju i inwestycji**, która w oparciu o wspólne ramy strategiczne definiowałaby priorytety inwestycyjne, przydział środków krajowych i unijnych na priorytetowe obszary i programy, jak również uzgodnione uwarunkowania oraz cele, jakie dane państwo zamierza osiągnąć. Umowa obejmowałaby politykę spójności i zastąpiłaby obecne Narodowe Strategiczne Ramy Odniesienia. Komisja uważa, że aby działania na rzecz spójności gospodarczej, społecznej i terytorialnej miały spójny i jednolity charakter, winna obejmować także inne polityki i instrumenty finansowe UE. Umowa taka stanowiłaby wynik rozmów między państwami członkowskimi i Komisją na temat strategii rozwoju UE i ich korelacji z krajowymi strategiami rozwoju.
- **programy operacyjne (PO)**, które podobnie jak w obecnej perspektywie stanowiłyby główne narzędzie zarządzania i które przekładałyby dokumenty strategiczne na konkretne priorytety w zakresie inwestycji wraz z przejrzystymi i dającymi się zmierzyć wskaźnikami sukcesu.

Kombinacja powyższych elementów powinna w opinii Komisji przyczynić się do osiągnięcia celów wyznaczonych dla krajów członkowskich w ramach strategii „Europa 2020". Sprawozdania roczne, śledzące postępy poczynione w ich realizacji, byłyby zsynchronizowane z cyklem zarządzania strategii „Europa 2020" i stałyby się podstawą regularnych debat politycznych na forum Rady obradującej w odpowiednich składach oraz komitetów Parlamentu Europejskiego, poprawiając w ten sposób przejrzystość i ocenę efektów polityki spójności, jak również zwiększając odpowiedzialność za jej efekty.

Trzy propozycje w przeglądzie budżetu UE są szczególnie ważne dla zmian polityki spójności.

Po pierwsze, Komisja uważa, że niezbędne jest, aby państwa członkowskie i regiony skoncentrowały zasoby krajowe i unijne na niewielkiej liczbie priorytetów stanowiących odpowiedź na konkretne wyzwania, z którymi należy się zmierzyć w kontekście krajowym i unijnym. Komisja chce to osiągnąć poprzez określenie w przepisach dotyczących strategii spójności ograniczonej liczby priorytetów tematycznych powiązanych ściśle z projektami przewodnimi zapowiedzianymi w strategii „Europa 2020". Trzeba tu niestety przypomnieć, że od czasu zaniechania projektu Narodowego Planu Rozwoju na lata 2007-2013 ciągle nie mamy wieloletniej, kroczącej strategii rozwoju kraju wysokiego poziomu, jaka jest niezbędna do skorelowania listy priorytetów krajowych z unijnymi.

Po drugie, w celu wsparcia nowego systemu zarządzania gospodarczego Komisja proponuje wprowadzenie przepisów

warunkujących, stanowiących zachętę do podejmowania reform. Innymi słowy państwa członkowskie byłyby zobowiązane przeprowadzić reformy potrzebne do zapewnienia efektywnego wykorzystania środków finansowych w obszarach strategii „Europa 2020" bezpośrednio związanych z polityką spójności, takich jak: ochrona środowiska, działania na rzecz modelu elastycznego rynku pracy i bezpieczeństwa socjalnego (flexicurity), edukacja, badania i innowacje.

Po trzecie w końcu, sankcje finansowe i zachęty związane z paktem stabilności i wzrostu (dotąd ograniczone do Funduszu Spójności) byłyby rozszerzone na pozostałe części budżetu unijnego. W przypadku nieprzestrzegania zasad Komisja sugeruje wprowadzenie zasady zawieszania lub anulowania części bieżących lub przyszłych płatności z budżetu UE, a także bezwarunkowego zamykania szczególnie nieefektywnie funkcjonujących osi priorytetowych i działań.

Komisja rozważa też inne instrumenty, które mogłyby zwiększyć skuteczność polityki spójności. Na przykład na poziomie UE mogłaby zostać ustanowiona specjalna rezerwa na wykonanie, będąca czynnikiem zachęcającym do osiągania założeń i celów strategii „Europa 2020" oraz powiązanych celów krajowych: w trakcie przeglądu śródokresowego wydzielona część budżetu byłaby alokowana na rzecz państw członkowskich i regionów, których programy wniosły największy – w odniesieniu do punktu wyjścia – wkład w realizację celów i założeń strategii „Europa 2020".

Takie bardziej strategiczne i ukierunkowane na wyniki podejście do polityki spójności wymaga lepszych i sprawniejszych systemów monitorowania i oceny. Wskaźniki dla wszystkich działań w UE miałyby być zdecydowanie bardziej jednolite, statystycznie wiarygodne, elastyczne i bezpośrednio powiązane z interwencjami w ramach polityki spójności, jak również być sprawnie gromadzone i upowszechniane. Wskaźniki i założenia miałyby być uzgadnianie w trakcie debaty nad dokumentami programowymi wraz ze wskaźnikami obligatoryjnymi odnoszącymi się do strategii „Europa 2020".

Takie bardziej rygorystyczne, ale i jednolite podejście ograniczałoby „swobodę kreowania" polityki spójności przez poszczególne kraje, ale właśnie dzięki bezpośredniemu przełożeniu skutkowałoby znacznym uproszczeniem proceduralnym.

Spójność terytorialna nowym paradygmatem

Komisja myśli nie tylko o zmianach finansowych. Dyskutowane przez szefów państw w styczniu na Konferencji w Brukseli wnioski z tzw. piątego raportu spójności (sprawozdania w sprawie spójności gospodarczej, społecznej i terytorialnej) wskazują na zapisy traktatu lizbońskiego. A on oprócz spójności gospodarczej i społecznej jako jeden z celów wymienia też **spójność terytorialną**. Z tego względu Komisja uważa, że nowe programy powinny również objąć ten cel, ze szczególnym uwzględnieniem roli miast, obszarów borykających się ze szczególnymi problemami geograficznymi i demograficznymi i polityki ponadregionalnej (makroregionów).

Komisja uważa, że obszary miejskie już stają się motorami wzrostu i platformami kreatywności i innowacji. Wyższy wzrost i nowe miejsca pracy powstają właśnie w miastach gdzie ma szanse zaistnieć masa krytyczna jednostek takich, jak przedsiębiorstwa, uniwersytety i naukowcy, a także nastawiona na rozwiązywanie konkretnych problemów administracja publiczna. Nie przypadkiem czołowe ośrodki badawcze i think-tanki przewidują, że to rozwój metropolii będzie istotnym

czynnikiem postępu technologicznego w najbliższych latach. **Metropolie będą w ich opinii szczególnym miejscem kształtowania się jakościowo nowych rozwiązań ICT nieograniczonych tylko do rozwiązań tzw. „inteligentnego miasta".** Problemy miast, ich mieszkańców i firm w nich działających, niezależnie od tego, czy dotyczą degradacji środowiska, czy wykluczenia społecznego, wymagają zdecydowanych rozwiązań i bezpośredniego zaangażowania organów właściwego szczebla. W związku z tym Komisja uważa, że nadszedł czas na przygotowanie ambitnych programów rozwoju europejskich metropolii, w których znaczące środki finansowe przekazane by zostały władzom metropolitalnym na projektowanie i wdrażanie skutecznych strategii rozwoju obszarów miejskich. Działania dotyczące miast, jak również stosowne środki i wybrane miasta powinny zostać jasno określone w dokumentach programowych.

Spójność terytorialna oznacza również wspieranie tworzenia powiązań między obszarami miejskimi i wiejskimi w kontekście dostępu do wysokiej jakości usług i infrastruktury, a także rozwiązywanie problemów regionów o wysokiej koncentracji grup marginalizowanych społecznie, zwłaszcza w kontekście zjawiska wykluczenia cyfrowego. Komisja uważa w tym kontekście za wskazane podjęcie prac nad strategiami i programami makroregionalnymi, tj. na obszarach statystycznych NUTS-1 (w Polsce obejmujących kilka województw). Warto przypomnieć, że takim programem makroregionalnym realizowanym w obecnej perspektywie jest PO Rozwój Polski Wschodniej.

Trzeba tu wspomnieć jeszcze o jednej ważnej propozycji Komisji wspieranej przez zdecydowaną większość UE-27: obecnie wsparcie regionów (nie tylko z instrumentów zaliczanych do funduszy strukturalnych) jest zależne od stopnia rozwoju gospodarczego regionu (mierzonego za pomocą PKB na mieszkańca). Istnieje wyraźny podział na regiony „mniej" i „bardziej" rozwinięte. Komisja uważa, że należy doprowadzić do bardziej sprawiedliwego traktowania regionów o podobnym poziomie i wprowadzić prostszy system wyznaczania regionów „pośrednich" w miejsce obecnego zawiłego podziału na tzw. regiony phasing-out i i phasing-in. W skład tej kategorii wchodziłyby również regiony obecnie kwalifikujące się do wsparcia w ramach celu „Konwergencja", których PKB byłby wyższy niż 75% średniej unijnej zgodnie z najnowszymi danymi statystycznymi. Wbrew pozorom jest to istotne dla Polski, bo wiele wskazuje, że w nowym okresie w Polsce mogą pojawić się tego typu „ubogacone" regiony (i to nie tylko Mazowsze, a zasadniczo Warszawa).

Co nas zatem czeka

Oczywiście od tych propozycji do realizacji jeszcze daleka droga (a zasadniczo długa dyskusja) i wypada poczekać na to, co przedstawi Komisja Europejska. Tym niemniej już teraz widać, że należy przygotować się na spore zmiany. Szanse utrzymania „wszystkiego jak jest" są nikłe, albowiem wiele krajów (i to niekoniecznie „starej Unii") popiera kierunek zmian. Nie wszystkie aktywności, które obecnie wspiera się z szeroko pojętych funduszy strukturalnych, pozostaną nimi, a i ogólne reguły owego wsparcia mocno się zmienią.

Należy podkreślić, że od czasu ogłoszenia strategii „Europa 2020" Komisja Europejska konsekwentnie stoi na stanowisku, że wszystkie krajowe programy operacyjne i finansowane z nich inwestycje będą musiały być ściśle dostosowane do celów strategii i jej inicjatyw kierunkowych.

Oznacza to, że zgodnie z celami strategii dotowane przez UE winny być tylko takie projekty, które są innowacyjne,

zapewniają rentowność oraz faktycznie wpływają na rozwój regionów i całej UE i ich mieszkańców. Odnosząc to do branży ICT, można wskazać na następujące obszary sygnalizowane zresztą konsekwentnie przez Komisję:

- Miejsce projektów budowy sieci „klasycznego", szerokopasmowego dostępu do Internetu (2 Mb/s) zajmą inicjatywy budowy tzw. sieci nowej generacji (NGN/NGA), umożliwiających dostęp klienta do Internetu z prędkością co najmniej 30 Mb/s.
- Promowane będą innowacyjne rozwiązania z obszaru eGovernment niesprowadzające się tylko i wyłącznie do prostego rozszerzenia usług administracji krajowej. Promowane będą systemy o dużym ładunku innowacyjności, o zasięgu transgranicznym i paneuropejskim, np. systemy wielojęzyczne, umożliwiające dostęp do usług administracji poprzez technologie mobilne w trybie 7/24 itp.
- Ważną rolę odgrywać będą projekty wspierające rozwój umiejętności cyfrowych we wszystkich grupach społecznych ze szczególnym podkreśleniem grup wykluczenia (w tym osób starszych, chorych i niepełnosprawnych).

Idąc tokiem rozumowania Komisji, należy spodziewać się, że większe nakłady zostaną prawdopodobnie przeznaczone na realizację projektów w ramach Europejskiego Funduszu Społecznego. Komisja sugeruje bowiem, ażeby znacząco większe środki z EFS były przeznaczane na wzmacnianie procesu edukacji w zawodach perspektywicznych, do których zaliczają się specjalności z grupy „teleinformatyka".

Natomiast jeśli chodzi o środki z Funduszu Spójności i w ramach Europejskiego Funduszu Rozwoju Regionalnego, Komisja zdecydowanie opowiada się za wprowadzeniem szerokiego systemu pożyczek i kredytów w miejsce obecnych bezzwrotnych dotacji. Co ciekawe, model ten stosowany byłby w większości przypadków także dla jednostek administracji: byłyby to niskooprocentowane kredyty spłacane w długiej skali czasowej z możliwością umorzenia – analogicznie jak pożyczki Banku Światowego (praktycznie dotacje przeznaczane byłby dla NGO's i instytucji społeczeństwa i obywatelskiego).

Nakreślone wyżej propozycje zmian są oczywiście jeszcze robocze. Tym niemniej nie należy traktować ich jako porażki „na dzień dobry", albowiem otworzą się nowe bardzo interesujące możliwości, zwłaszcza dla branży ICT, związane np. ze wspieraniem obszarów metropolitalnych czy tworzeniem zintegrowanych programów infrastrukturalnych dla makroregionów. Będzie to duże wyzwanie dla potencjalnych beneficjentów oraz dla firm, które będą ich wspierały.

Abstract

Support for the ICT in the new EU financial perspective

In June 2011 the proposal of the new financial perspective (multi-annual plan for the Community budget for years 2014-2020) will be presented by European Commission. The article discusses the opportunities and threats for the Polish ICT Industry in the context of planned changes indicated by the Commission. The article especially focuses on the analysis of the consequences of changes in the to the regional policy area (and so-called EU structural funds) according to the Europe 2020 strategy and its key initiatives with an emphasis on "Digital Agenda for Europe".

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

E-dowód osobisty - projekt zmian w ustawie o dowodzie osobistym

Mirosław Kutyłowski

W projekcie z dnia 12.04.2011 Ministerstwo Spraw Wewnętrznych i Administracji proponuje zmiany w ustawie o dowodzie osobistym. Biorąc pod uwagę rozmiar tekstu nowelizacji, można by odnieść wrażenie, że chodzi o zmiany kosmetyczne. W istocie mamy tu do czynienia z zupełnie inną koncepcją dowodu osobistego, prawie pozbawionego funkcji elektronicznych. Zamiast innowacyjnego dowodu osobistego proponuje się rozwiązania sprawdzone w praktyce – stosunkowo łatwe do implementacji, ale, jak uczy przykład innych państw, o znikomej użyteczności dla państwa i obywateli. Co więcej, są to rozwiązania przestarzałe pod względem poziomu bezpieczeństwa. Kontrowersyjny wydaje się również sam termin wprowadzenia e-dowodu w okrojonej postaci – całkowita zmiana koncepcji tak dużego systemu powoduje, że wiele prac, które już powinny być wykonane, należy rozpocząć od nowa.

Warstwa elektroniczna dowodu osobistego miała służyć kilku celom:

1. Zapisanie danych z warstwy graficznej w (chronionej) warstwie elektronicznej i możliwość porównania tych danych. Daje to lepsze możliwości zabezpieczenia dowodu osobistego przed manipulacjami (zmiana danych w autentycznym dowodzie osobistym) – fałszerz musiałby nie tylko przełamać zabezpieczenia graficzne (co jest możliwe przynajmniej w wypadku najbardziej zaawansowanych technologii fałszerskich), jak i kryptograficzne (co nie należy do bieżącego stanu techniki).
2. Możliwość zdalnego uwierzytelniania obywatela poprzez fizyczne użycie dowodu osobistego. Wykorzystujemy tu fakt, że z innych względów (np. możliwość pobrania kredytu gotówkowego) dowód osobisty nie jest udostępniany osobom trzecim. Sprawdzenie obecności dowodu osobistego wymaga oczywiście użycia silnych (lecz dziś standardowych) metod kryptograficznych.
3. Umożliwienie uwierzytelniania się w niektórych systemach z zachowaniem anonimowości (*ograniczona identyfikacja*). Rozwiązanie to ma umożliwiać ochronę danych osobowych na poziomie technicznym i rezygnację z identyfikacji osoby tam, gdzie nie jest to konieczne (lub wręcz stanowi poważne zagrożenie).
4. Umożliwienie opatrywania zaawansowanym podpisem elektronicznym dokumentów przedkładanych podmiotom publicznym przez obywateli w sposób niepowodujący istotnych kosztów i uciążliwości po stronie obywatela, jednak zapewniający pewność obrotu po stronie administracji publicznej, nawet w przypadku osłabienia mechanizmów kryptograficznych.
5. Próba ratowania rynku podpisów kwalifikowanych (w języku obecnie obowiązującej ustawy: *bezpiecznych podpisów elektronicznych weryfikowanych ważnym kwalifikowanym certyfikatem*) poprzez dostarczenie przez państwo bezpiecznych urządzeń do składania podpisu elektronicznego.
6. Wykorzystanie dowodu osobistego jako ezpiecznego komponentu systemu elektronicznego dla e-zdrowia, w szczególności zapewniającego odpowiednie narzędzia kryptograficzne.

Uwierzytelnianie

Projekt pozostawia w warstwie deklaratywnej mechanizmy uwierzytelnienia: *dowód osobisty umożliwia uwierzytelnienie go w systemach teleinformatycznych podmiotów publicznych, uwierzytelnienie jego posiadacza w systemach teleinformatycznych*.

Zasadniczą zmianą jest projektowany zapis „w art. 18 uchyla się ust. 5", ten zaś określa jedno z pól certyfikatu dowodu osobistego jako *dane służące do weryfikacji informacji uwierzytelniającej*. W języku technicznym to pole certyfikatu oznacza po prostu klucz publiczny do weryfikacji *informacji uwierzytelniającej*, czyli danych generowanych przez dowód osobisty w ramach protokołu uwierzytelniania.

Niejasne są zamiary takiej zmiany. W grę mogą wchodzić następujące scenariusze:

1. Zastąpienie silnych mechanizmów uwierzytelniania przez atrapy w rodzaju kodów MAC dla danych umieszczonych w dowodzie osobistym lub hasła. Wadą tych rozwiązań (dawno zarzuconych np. w przypadku e-paszportów) jest łatwość w klonowaniu dowodów osobistych – dane te są bowiem podawane tekstem jawnym przy odczycie. Weryfikacja takich danych nie daje zatem żadnej pewności obecności dowodu osobistego, a tym samym uwierzytelniania posiadacza. Sprawdzenie poprawności kodu ze względu na stosowane techniki symetryczne albo nie daje żadnych gwarancji (poza korekcją błędu), albo wymaga kontaktu online w celu sprawdzenia kodu w centralnej bazie danych.
2. Oparcie uwierzytelnienia o przedstawienie danych z warstwy elektronicznej pieczęcią elektroniczną organu wydającego dowód osobisty. Rozwiązanie to może być nawet słabsze od poprzedniego, bo umożliwia atak typu replay: osoba wobec której obywatel X się uwierzytelnił, może uwierzytelniać się jako X.
3. Oparcie się o techniki *IBC* lub *certificate--less* pozwala na rezygnację z certyfikatu, jednak rozwiązania takie według mojej wiedzy nie są stosowane dla dokumentów identyfikacyjnych przez żaden z krajów UE. To w konsekwencji może spowodować kłopoty z używaniem polskich dokumentów w sposób elektroniczny za granicą.

   Generowanie kluczy prywatnych jest w przypadku tych schematów uciążliwe, gdyż jest dokonywane przy intensywnym udziale serwera KGC. Dla schematów tych wymaga się pełnego zaufania do KGC – bowiem jest on w stanie tworzyć klucze dla kart posługujących się tym samym identyfikatorem (łatwe klonowanie dowodów osobistych przez wystawcę). Zatem z punktu widzenia praktycznych uwarunkowań jest to raczej rozwiązanie czysto akademickie.

Żadne z powyższych rozwiązań nie prowadzi do budowy poprawnie funkcjonującego systemu uwierzytelniania. Uzasadnienie do projektu nie zawiera żadnych wskazówek, co autorzy regulacji zamierzają osiągnąć i w jaki sposób.

Ograniczona identyfikacja

Projekt usuwa z ustawy wszelkie odniesienia do ograniczonej identyfikacji, blokując na drodze prawnej zaimplementowanie tych mechanizmów w dowodzie osobistym, w tym usuwając wprost możliwość uwierzytelniania się bez ujawnienia tożsamości.

Uzasadnienie projektu powołuje się na brak dostępnych rozwiązań technicznych oraz kontrowersje związane z wprowadzaniem tego rozwiązania w Niemczech. Obie informacje są nierzetelne.

Co prawda metody ograniczonej identyfikacji nie osiągnęły stanu, który moglibyśmy określić jako brak dalszych postępów technologii, jednak sytuacja ta dotyczy większości technologii w tej dziedzinie. W szczególności dotyczy to kart chipowych, gdzie zmiany technologiczne są tak szybkie, że rozwiązania oparte o standardy są zazwyczaj przestarzałe z technicznego punktu widzenia.

Najprostsze rozwiązanie dla ograniczonej identyfikacji polega na użyciu odrębnej pary kluczy dla uwierzytelniania metodami kryptografii asymetrycznej – lecz w oparciu

o certyfikat nieidentyfikujący osoby posługującej się tym certyfikatem. Jest to rozwiązanie znane od kilkudziesięciu lat.

Istotne wyzwania zaczynają się wtedy, gdy zamierzamy wykorzystać ten sam klucz prywatny do ograniczonej identyfikacji w nieograniczonej z góry liczbie sektorów. Rozwiązanie wspomniane powyżej możliwe jest tylko dla bardzo niewielkiej liczby sektorów ze względu na pojemność pamięci – obecnie najbardziej deficytowego zasobu na kartach kryptograficznych. Rozwiązanie, które umożliwia wykorzystanie tego samego klucza prywatnego do nieograniczonej liczby sektorów, z zachowaniem tzw. *unlinkability* pomiędzy sektorami, zostało wdrożone w nowym, niemieckim dowodzie osobistym i funkcjonuje na kilku milionach już wydanych dowodów osobistych. Rozwiązanie to trudno określić jako wzbudzające kontrowersje w Niemczech – zostało ono pozytywnie przyjęte zarówno przez organy odpowiedzialne za ochronę danych osobowych, jak i organizacje pozarządowe. Było natomiast atakowane przez koncerny nieposiadające własnych rozwiązań tego typu.

Nie jest oczywiste, czy należy wykorzystać dokładnie rozwiązanie niemieckie – w przypadku zastosowań takich jak NFZ bardziej wskazane jest oparcie się o tzw. *whitelists* (lista uprawnionych kluczy publicznych) niż o *blacklists* (lista zablokowanych kluczy publicznych). Odpowiednie rozwiązanie zbudować można w oparciu o te same komponenty kryptograficzne co rozwiązanie niemieckie. Co więcej, rozwiązanie takie posiada również formalny dowód bezpieczeństwa. Możliwe jest również wykorzystanie koncepcji zaufanej trzeciej strony – rozwiązania opracowanego przez jedną z firm francuskich. Jest to rozwiązanie oparte o techniki symetryczne i posiada wszystkie wady i zalety udzielania dostępu w oparciu o atrybuty posiadacza dowodu osobistego.

Wybór rozwiązania najbardziej odpowiadającego polskim potrzebom zależy od określenia pola zastosowań. Na pewno należy tu zwrócić uwagę na tzw. *killer applications*. Niewątpliwie jest kilka kategorii zastosowań, gdzie ograniczona identyfikacja może zrewolucjonizować zwalczanie patologii. Dotyczy to na przykład zgłaszania zagrożeń bezpieczeństwa w zakładach pracy do organów kontrolnych (takich jak np. manipulacje sensorów wykrywających zagrożenie metanem w kopalniach). Obecnie problem polega na tym, że tożsamość osoby zgłaszającej nieprawidłowości może zostać przekazana pracodawcy, a w konsekwencji może powodować zwolnienie z pracy informatora pod jakimś pretekstem. W pełni anonimowy kanał zabezpiecza osobę informującą, a jednocześnie daje gwarancje organowi przyjmującemu zgłoszenie, że pochodzi ono od osoby fizycznej. Ponadto w przypadku użycia odpowiedniej techniki umożliwia sprawdzenie, czy dwie różne informacje pochodzą od tej samej osoby. Pomaga to we wstępnej ocenie wartości zgłoszenia.

Podobne scenariusze wykorzystania ograniczonej identyfikacji byłyby niezwykle cenne dla zwalczania przestępczości (ochrona świadków na drodze elektronicznej), a także dla ochrony nieletnich. W ostatnim przypadku chodzi o stworzenie kanału komunikacji w sytuacjach bardzo trudnych psychologicznie dla poszkodowanych.

Na obecnym etapie nie widać powodów, dla których należałoby usunąć ograniczoną identyfikację z dowodu osobistego. Wręcz przeciwnie, należałoby zdefiniować zakres prac pozwalających na implementację rozwiązania w przeciągu kilku lat. Przy takim podejściu celowe wydaje się określenie daty wprowadzenia ograniczonej identyfikacji na drodze delegacji ustawowej przy jednoczesnym zobowiązaniu politycznym i określenia planu tych prac (czyli *roadmap* w modnej dziś terminologii).

Podpis osobisty

Obowiązująca ustawa mówi, że podpis osobisty to zaawansowany podpis elektroniczny (wg definicji Dyrektywy UE), który jest sporządzony przy pomocy klucza prywatnego znajdującego się w dowodzie osobistym i *uzupełniony przez ministra właściwego do spraw wewnętrznych danymi pozwalającymi na określenie czasu złożenia tego podpisu*. Projekt proponuje wykreślenie tej ostatniej frazy.

Konsekwencją tej zmiany jest rezygnacja z gwarancji bezpieczeństwa dla podpisu osobistego. Zasadniczą zaletą obowiązującej wciąż regulacji jest:

- odmowa „uzupełnienia" w przypadku, gdy dowód osobisty jest na liście unieważnionych dokumentów,
- stosowanie monitoringu bezpieczeństwa (podobnego jak w przypadku kart kredytowych) i stosowanie elastycznych polityk bezpieczeństwa (np. zablokowanie na czas wyjazdu na wakacje),
- potwierdzanie czasu złożenia podpisu, a tym samym uniemożliwienie antydatowania dokumentów,
- ominięcie pięty achillesowej podpisów kwalifikowanych, polegającej na trudności określenia statusu prawnego podpisu – podpis taki jest ważny jedynie, gdy został złożony w okresie ważności kwalifikowanego certyfikatu, czego jednak sam podpis kwalifikowany nie pozwala sprawdzić; „uzupełnianie" daje jednoznaczność stanu prawnego wynikającą z samego podpisu,
- uproszczenie procesu weryfikacji podpisu i eliminacja konieczności kontaktu online.

Oczywiście realizacja warunku z ustawy wymaga pewnego minimalnego choćby serwisu po stronie systemu PL.ID (jest to również konieczne dla systemu po zaproponowanych zmianach). Z drugiej strony redukuje to koszty procedowania dokumentów elektronicznych w urzędach, zwiększa pewność obrotu i zabezpiecza przed atakami.

Uzasadnienie do projektu zawiera argument, że przepis ustawy wskazuje na konieczność zastosowania techniki podpisu z mediatorem. Argument jest chybiony, proces może być zrealizowany przez następujący trywialny w implementacji protokół.

Krok 1: dowód osobisty generuje podpis elektroniczny s pod dokumentem M w dowolny sposób, jedno z pól podpisu określa moment złożenia podpisu t. Uwaga: podpis s nie jest przekazywany poza dowód osobisty.

Krok 2: dowód osobisty szyfruje s przy pomocy klucza publicznego serwera PL.ID, wynikowy kryptogram c jest przekazywany do aplikacji komunikującej się z dowodem osobistym.

Krok 3: aplikacja przesyła kryptogram c do serwera PL.ID.

Krok 4: serwer PL.ID deszyfruje c, korzystając z własnego klucza prywatnego i odzyskuje s. Następnie serwer:

1. sprawdza, czy dowód osobisty wskazany w podpisie nie został zastrzeżony (lub czy nie jest zablokowany do składania podpisu w chwili t); jeśli został zastrzeżony, to dalsze kroki nie są wykonywane (a raczej wykorzystywana jest informacja o próbie użycia zastrzeżonego dowodu osobistego),
2. sprawdza, czy czas t wskazany w podpisie różni się od czasu serwera o nie więcej niż pewną wartość Δ; jeśli granica ta jest przekroczona, to dalsze kroki nie są wykonywane i zwracana jest informacja o błędzie,
3. weryfikuje podpis w sensie kryptograficznym, korzystając z kryptograficznego skrótu dokumentu klucza publicznego osoby podpisującej oraz z podpisu s; jeśli weryfikacja da wynik negatywny, to dalsze kroki nie są wykonywane i zwracana jest informacja o błędzie.

Krok 5: serwer przesyła s do aplikacji.

Aby ustrzec się przed podsłuchiwaniem i zdobyć pewność, że podpis jest istotnie wykonywany przez dowód osobisty, na wstępie może zostać nawiązana łączność za pomocą standardowego protokołu Chip Authentication i wymianę danych prowadzić kanałem zaszyfrowanym kluczem efemerycznym.

Realizacja podpisu osobistego jako podpisu z mediatorem jest rozwiązaniem, które zapewnia wysoki poziom bezpieczeństwa w sytuacji, gdy nie można w pełni zawierzyć dostawcy części elektronicznej dowodu osobistego. Należy tu jeszcze dodać, że efektywna realizacja podpisu z mediatorem możliwa jest zarówno w oparciu o problem faktoryzacji (podpisy RSA), jak i w oparciu o dyskretny logarytm (w szczególności dla arytmetyk realizowanych na krzywych eliptycznych).

Uzasadnienie projektu wskazuje na zamiar oparcia podpisu osobistego o listy CRL i usługę OCSP, tak jak ma to miejsce w przypadku podpisu kwalifikowanego. Pod względem technicznym stwarza to same kłopoty. W przypadku procedowania dokumentu elektronicznego opatrzonego podpisem osobistym (na przykład w gminie) niezbędne będzie odwoływanie się do list CRL lub usługi OCSP. W pierwszym wypadku mamy do czynienia z uciążliwościami związanymi ze ściąganiem do każdej jednostki administracji publicznej w Polsce list CRL. Brak dotychczas praktycznych realizacji tej skali i można obawiać się zatkania systemu. Druga możliwość (OCSP) oznacza konieczność podłączenia każdej jednostki publicznej w Polsce szybkim łączem do Internetu. Oznacza to również niemożność procedowania w przypadku awarii łączności – nie sposób bowiem sprawdzić, czy pismo zostało opatrzone podpisem tak jak wymaga tego Kodeks Postępowania Administracyjnego. Dodajmy, że podpis osobisty miał przede wszystkim stanowić ułatwienie dla podmiotów publicznych, a przy takiej technologii staje się sporą uciążliwością.

Problemy nie kończą się w tym miejscu. Pamiętać trzeba również o sporej liczbie kradzieży dowodów osobistych. W przypadku podpisu osobistego aktywowanego na dowodzie usługa OCSP jest dla złodzieja znakomitym narzędziem służącym do sprawdzenia, czy dowód osobisty został już zastrzeżony. Dzięki temu złodziej może ograniczyć ryzyko w posługiwaniu się skradzionym dowodem osobistym. Ze względu na bezpieczeństwo osobiste wypada więc doradzić posiadaczowi nieaktywowanie podpisu osobistego!

Najistotniejszym efektem proponowanych zmian wydaje się praktyczna eliminacja podpisu osobistego i utrzymanie monopolu dla podpisu kwalifikowanego.

Podpis kwalifikowany

Proponowane zmiany nie dotyczą podpisu kwalifikowanego, pomimo że jest to najbardziej kontrowersyjna i najmniej użyteczna dla państwa część dowodu, a zarazem najtrudniejsza w implementacji. Problemem jest to, że uprawnienie do zainstalowania podpisu kwalifikowanego uzyskują wyłącznie podmioty kwalifikowane. Dotyczy to jednak nie tylko podmiotów zarejestrowanych w Polsce, ale wszelkich podmiotów kwalifikowanych z Europejskiego Obszaru Gospodarczego. Sprawdzenie statusu danego podmiotu nie jest do końca trywialne, jednak najtrudniejsze okazuje się zagwarantowanie kontroli przez dowód osobisty, komu udziela prawa do zapisu danych w swojej pamięci. Niemcy zbudowali w tym celu system oparty na certyfikatach dostępu.

Oczywiście można się obawiać, że obszar zarezerwowany dla podpisu kwalifikowanego będzie otwarty dla każdego. Wtedy niestety musimy się liczyć z próbami zainstalowania w dowodzie osobistym takich danych, które mogą służyć do ataku na dowód lub danych do wykorzystania dowodu w sposób sprzeczny z prawem, lub rozszerzenia o funkcjonalności

nieprzewidziane ustawą. W ten sposób państwo utraciłoby kontrolę nad zawartością warstwy elektronicznej dowodu osobistego.

Karta ubezpieczenia zdrowotnego

Proponowane zmiany wyłączają możliwość budowy Karty Ubezpieczenia Zdrowotnego (KUZ) z wykorzystaniem wspólnych mechanizmów kryptograficznych z dowodem osobistym – po prostu z dowodu osobistego one znikają.

Fundamentalnymi mechanizmami dla KUZ wydają się w chwili obecnej:

1. Możliwość uwierzytelnienia się elektronicznie wobec terminala świadczącego usługi medyczne (świadczący usługę uzyskuje pewność co do autentyczności uprawnienia do uzyskania usługi) - w języku technicznym chodzi o tę czy inną formę protokołu Chip Authentication.
2. Możliwość weryfikacji przez KUZ tego, że komunikacja prowadzona jest z uprawnionym terminalem świadczącego usługi medyczne - w języku technicznym chodzi o tę czy inną formę protokołu Terminal Authentication.
3. Możliwość tworzenia tokenów uwierzytelniających transakcje i przekazywania ich bezpiecznym kanałem do ubezpieczyciela.
4. Możliwość silnego kryptograficznie uwierzytelniania w celu uzyskania dostępu do własnych danych medycznych w sposób nieumożliwiający identyfikacji – tj. przy pomocy ograniczonej identyfikacji.

Proponowane zmiany eliminują standardowe narzędzia w e-dowodzie, którymi zadania te byłyby realizowane. Tak więc na przykład ograniczona identyfikacja będzie musiała być zaimplementowana (o ile to w ogóle okaże się wykonalne w zamówionym chipie) osobno w obszarze KUZ, bez możliwości wykorzystania tego kodu dla innych celów. Wynika to ze specyfiki systemów operacyjnych bezpiecznych kart chipowych.

Perspektywy e-ID w Polsce

Redukcja funkcjonalności PL.ID każe zadać sobie pytanie, jak odpowiadające im zadania będzie można zrealizować:

- Z pozoru nienaruszone jest zastosowanie dowodu osobistego jako nośnika dla podpisu kwalifikowanego. Jednak i tu należy mieć poważne wątpliwości, czy e-dowód osobisty okaże się pomocny. Jakkolwiek osoba posługująca się podpisem kwalifikowanym nie będzie musiała nabywać karty kryptograficznej – jako bezpiecznego urządzenia do składania podpisu elektronicznego - jednak jest to oszczędność w istocie kilku lub kilkunastozłotowa.
  Istotne oszczędności uzyskać można wtedy, gdy instalacja podpisu osobistego odbywa się zdalnie, włącznie z weryfikacją tożsamości składającego wniosek. To bardzo mocno powinno zredukować koszty certyfikatów kwalifikowanych oraz uciążliwości dla podpisującego (eliminacja konieczności osobistego stawienia się w punkcie rejestracji). Silne uwierzytelnienie dowodu osobistego i pewność usługodawcy, że instaluje podpis kwalifikowany w dowodzie osobistym będącym *bezpiecznym urządzeniem do składania podpisu elektronicznego,* zmniejszają poziom ryzyka, a tym samym koszty usługodawcy.
  O ułatwieniach tych można mówić w przypadku nowego niemieckiego dowodu osobistego, ale już nie w przypadku e-dowodu po proponowanych zmianach. Inną rzeczą jest to, czy reanimacja podpisu kwalifikowanego w Niemczech okaże się skuteczna. W to też można wątpić.
- Rezygnacja z uwierzytelniania w e-serwisach publicznych za pomocą e-dowodu każe zastanowić się, w jaki sposób problem uwierzytelniania zostanie rozwiązany. Problem nie jest czysto techniczny, ale również formalno-prawny: powstanie rozwiązań opartych o *federated identity management* w sektorze publicznym wymaga zdefiniowania kompetencji i uprawnienia

do świadczenia takich usług. Obecny stan prawny (ustawa o podpisach elektronicznych) takich usług nawet zabrania. Jedynym realistycznym rozwiązaniem o charakterze ogólnodostępnym pozostaje usługa ePUAP – pod względem technicznym uproszczona (i mniej bezpieczna) wersja rozwiązań duńskich.
W sytuacji takiej należy się spodziewać budowy lokalnych rozwiązań na własne potrzeby przez poszczególne resorty, samorządy itp.

- Karta ubezpieczenia zdrowotnego bez wsparcia o mechanizmy bezpieczeństwa dowodu osobistego traci swój pierwotny sens. W tej sytuacji łatwiej, bezpieczniej i taniej mogłoby okazać się zbudowanie odrębnej karty z silnymi mechanizmami w rodzaju ograniczonej identyfikacji wbudowanych efektywnie na poziomie systemu operacyjnego.

Prywatyzacja dowodu osobistego

Google, Facebook, Twitter zrewolucjonizowały funkcjonowanie sieci pod względem oferowanych usług dla osób fizycznych. W działaniu tych serwisów widać nieustanny postęp w oferowaniu pożytecznych rozwiązań, innowacyjność i pragmatyzm.

Niebawem może okazać się, że serwisy te oferują wsparcie w zakresie elektronicznej identyfikacji i e-dowody tożsamości, przejmując tradycyjne obszary zastrzeżone dla państwa. Akceptacja takich dokumentów może się rozwijać bardzo szybko w obrocie cywilnym – ze względu na swą olbrzymią wiedzę o osobach fizycznych serwisy te są w stanie zagwarantować dużo lepszą kontrolę nad wydawaniem dokumentów tożsamości, niż są to w stanie uczynić organy publiczne. Z tego względu może okazać się, że na przykład uzyskanie kredytu będzie za kilka lat trudniejsze (i droższe) w przypadku posługiwania się państwowym dowodem osobistym niż w przypadku e-dowodu wydawanego przez prywatną firmę. Co zrobimy, gdy możliwość wjazdu bezwizowego do pewnych krajów uzależniona zostanie od posiadania tego typu dokumentu tożsamości?

Taki rozwój sytuacji, być może korzystny z punktu widzenia wygody obywatela, nie musi być jednak korzystny dla interesów państwa. Słaby pod względem funkcjonalności dowód osobisty nie będzie jednak mógł konkurować z „prywatnym" dowodem osobistym wydawanym przez zagraniczne firmy.

Abstract

E-ID card - proposed changed to Polish law on personal identity cards

Recently, Polish Ministry of Interior and Administration proposed changes to the current law concerning personal identity cards equipped with electronic layer. The proposed changes are fundamental for the electronic layer and cancel most of the functions planned so far. This concerns in particular:

- removing public keys for e-ID card authentication from the e-ID card,
- removing possibility to authenticate himself with an e-ID card without disclosing own identity (restricted identification),
- removing the requirement for personal signature saying that a trusted server run by the state must participate in signature creation confirming the signing time and preventing signature creation with revoked or stolen E-ID cards.

We describe security flaws, dangers and usability consequences, among others for applying e-ID as a health insurance card.

Prof. Mirosław Kutyłowski - pracownik Instytutu Matematyki i Informatyki Politechniki Wrocławskiej, specjalista w zakresie algorytmów i zagadnień bezpieczeństwa komputerowego.

Prawo do bycia zapomnianym

Arwid Mednis

W dniu 4 listopada 2010 r. Komisja Europejska opublikowała komunikat do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego oraz Komitetu Regionów pt. „Całościowe podejście do kwestii ochrony danych osobowych w Unii Europejskiej". Komunikat stanowi kolejny etap rozpoczętego w 2009 roku przeglądu europejskich ram prawnych ochrony danych osobowych. Jednym z poruszonych w dokumencie zagadnień jest poprawa kontroli nad własnymi danymi. Komisja podkreśla, że skuteczna kontrola nad danymi jest obok zasady minimalizacji (adekwatności) danych jednym z warunków wysokiego poziomu ochrony danych. Wśród wniosków odnośnie poprawy kontroli nad danymi Komisja deklaruje zbadanie tzw. prawa do bycia zapomnianym, tzn. *„prawa osób fizycznych do spowodowania usunięcia ich danych oraz zaprzestania ich przetwarzania, jeżeli przestały być potrzebne do zgodnych z prawem celów"*. Komisja podaje jako przykład cofnięcie uprzednio udzielonej zgody lub upływ okresu przechowywania danych.

Tak ogólnikowo sformułowany opis uprawnienia budzi szereg wątpliwości. Kontekst proponowanych zmian jest dość oczywisty: dotychczasowe instrumenty prawne okazują się niewystarczające wobec coraz większej dostępności naszych danych osobowych w sieci. Zagadnieniem wymagającym szczególnej uwagi jest fakt, że coraz większa część dotyczących nas danych nie pochodzi od nas samych. Należy spodziewać się rozwoju narzędzi analizujących dane z różnych źródeł i dostarczających przetworzone i wzbogacone informacje na nasz temat. Kontrola nad własnymi danymi będzie więc coraz trudniejsza. W szczególności coraz trudniejsze będzie doprowadzenie do usunięcia danych z sieci.

Prawo do zapomnienia obejmowałoby możliwość żądania usunięcia danych. Czy jednak jesteśmy w stanie stworzyć skuteczny instrument prawny, którego użycie spowoduje natychmiastowe zniknięcie danych z sieci? Istnieje niestety uzasadniona obawa, że wobec technicznych, psychologicznych i społecznych uwarunkowań funkcjonowania ludzi w cyberprzestrzeni nawet najbardziej rygorystyczne przepisy pozostaną martwe. Zagadnienie jest kompleksowe i wymaga z jednej strony wyważenia potrzeb i interesów, w tym ponownego określenia prywatności w hierarchii potrzeb jednostki, z drugiej strony – analizy wszystkich aspektów technicznych, a w szczególności informatycznych.

W dalszej części tekstu oprócz przypomnienia aktualnych ram prawnych kontroli nad danymi osobowymi chciałbym podzielić się kilkoma refleksjami na powyższe tematy. Przedstawię również wstępne uwagi związane z propozycją sformułowania prawa do bycia zapomnianym.

I.

Dyrektywa 95/46/WE[1] przewiduje kilka instrumentów, przy pomocy których jednostka sprawuje kontrolę nad swoimi danymi osobowymi. Są wśród nich:

1 Dyrektywa 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 (Dz. U. UE L z dnia 23 listopada 1995 r. ze zm.)

i) prawo dostępu do danych polegające m. in. na możliwości żądania sprostowania, usunięcia lub zablokowania danych, których przetwarzanie jest niezgodne z przepisami dyrektywy, szczególnie ze względu na niekompletność lub niedokładność danych (art. 12) oraz
ii) prawo sprzeciwu (art. 14).

Zgodnie z Dyrektywą to ostatnie uprawnienie powinno obejmować możliwość wniesienia przez jednostkę:

a) sprzeciwu co do przetwarzania dotyczących jej danych co najmniej w przypadkach wymienionych w art. 7 lit. e) i f)[2] Dyrektywy. Sprzeciw może zostać wyrażony w dowolnym czasie z ważnych i uzasadnionych przyczyn wynikających z konkretnej sytuacji danej osoby. Ustawodawstwo krajowe może odmiennie kształtować warunki zgłoszenia sprzeciwu tego rodzaju. W przypadku uzasadnionego sprzeciwu przetwarzanie danych przez administratora danych nie może już obejmować tych danych.
b) sprzeciwu, na wniosek i bez opłaty, wobec przetwarzania dotyczących jej danych osobowych dla potrzeb marketingu bezpośredniego lub żądania bycia poinformowanym przed ujawnieniem danych osobowych po raz pierwszy osobom trzecim lub ich wykorzystaniem w ich imieniu dla potrzeb marketingu bezpośredniego, jak również prawo wyraźnego powoływania się na prawo sprzeciwu, bez opłat, wobec ujawniania lub wykorzystywania danych.

Istotnym elementem kontroli jednostki nad własnymi danymi jest obowiązek informacyjny. Dyrektywa nakazuje poinformowanie tylko o prawie sprzeciwu wobec przetwarzania danych dla celów marketingu bezpośredniego, o którym mowa w lit. b) powyżej.

Powyższe uprawnienia zostały implementowane w polskiej ustawie o ochronie danych osobowych („UODO") w art. 32.

Zgodnie z polską ustawą jednostka ma zatem prawo żądania uzupełnienia, uaktualnienia, sprostowania danych osobowych, czasowego lub stałego wstrzymania ich przetwarzania lub ich usunięcia, jeżeli są one niekompletne, nieaktualne, nieprawdziwe lub zostały zebrane z naruszeniem ustawy albo są już zbędne do realizacji celu, dla którego zostały zebrane (art. 32 ust. 1 pkt 6 UODO).

Ponadto ma prawo:

a) wniesienia, w przypadkach wymie-

2 Chodzi o przesłanki legalności przetwarzania danych osobowych, a więc to, że dane mogą być przetwarzane tylko wtedy, gdy:

„e) przetwarzanie danych jest konieczne dla realizacji zadania wykonywanego w interesie publicznym lub dla wykonywania władzy publicznej przekazanej administratorowi danych lub osobie trzeciej, przed którą ujawnia się dane lub

f) przetwarzanie danych jest konieczne dla potrzeb wynikających z uzasadnionych interesów administratora danych lub osoby trzeciej, lub osobom, którym dane są ujawniane, z wyjątkiem sytuacji, kiedy interesy takie podporządkowane są interesom związanym z podstawowymi prawami i wolnościami osoby, której dane dotyczą, a które wymagają ochrony na podstawie art. 1 ust. 1." (w szczególności prawo do prywatności w odniesieniu do przetwarzania danych osobowych – przyp. AM)

nionych w art. 23 ust. 1 pkt 4 i 5[3], pisemnego, umotywowanego żądania zaprzestania przetwarzania jej danych ze względu na jej szczególną sytuację (art. 32 ust. 1 pkt 7),

b) wniesienia sprzeciwu wobec przetwarzania jej danych, w przypadkach wymienionych w art. 23 ust. 1 pkt 4 i 5, gdy administrator danych zamierza je przetwarzać w celach marketingowych lub wobec przekazywania jej danych osobowych innemu administratorowi danych (art. 32 ust. 1 pkt 8).

Skutkiem żądania zaprzestania przetwarzania danych lub wniesienia sprzeciwu jest co do zasady zaprzestanie ich wykorzystywania.

Administrator danych jest obowiązany poinformować osobę, której dane dotyczą, o powyższych uprawnieniach w przypadku, gdy otrzymał informacje od osoby trzeciej.

Analiza przepisów UODO wskazuje, że kontrola jednostki nad jej danymi prowadząca w szczególności do usunięcia tych danych jest w gruncie rzeczy dość ograniczona. Składa się na to kilka czynników, m. in.:

- administrator jest zobowiązany do usunięcia danych, jeśli zebrano je z naruszeniem przepisów lub gdy został zrealizowany cel, dla którego je zebrano. Nie można zatem, co oczywiste, domagać się usunięcia danych zebranych na podstawie ustawy lub w celu realizacji umowy, przynajmniej do czasu zrealizowania celu przetwarzania (określonego w ustawie, a w przypadku umowy do jej zakończenia, wliczając w to również okres przedawnienia roszczeń). Nie jest jasne, czy na takich samych zasadach co do skutków należy traktować cofnięcie zgody (do niedawna nie było nawet jasne, czy na gruncie UODO cofnięcie zgody jest dopuszczalne, obecnie kwestia ta jest przesądzona w ustawie). Wydaje się, że cofnięcie zgody powinno co do zasady skutkować usunięciem danych lub zaprzestaniem ich przetwarzaniem dla celu objętego zgodą (w przypadku gdy te same dane przetwarza się dla kilku różnych celów objętych różnymi przesłankami legalności).
- zarówno prawo żądania zaprzestania przetwarzania danych, jak i prawo sprzeciwu dotyczą wyłącznie przetwarzania danych opartego na przesłance wykonywania zadań dla dobra publicznego lub usprawiedliwionego celu. Żądania ani sprzeciwu nie można wnieść w sytuacji, gdy dane są przetwarzane na podstawie przepisów prawa lub w celu realizacji umowy. Żądanie zaprzestania przetwarzania danych trzeba umotywować szczególną sytuacją, sprzeciw z kolei jest skuteczny tylko wobec określonych celów przetwarzania.

II.

Wymienione powyżej uprawnienia nabierają szczególnego znaczenia wobec rozwoju nowoczesnych technologii, a w szczególności wymiany informacji w Internecie. Najważniejszą cechą aktualnych usług w sieci określanych wspólnie jako Web 2.0 jest globalny dostęp do informacji. Internet we wcześniejszym stadium nie gwarantował

3 Chodzi tu o przesłanki legalności przetwarzania danych osobowych odpowiadające cytowanemu powyżej art. 7 lit. e) i f) Dyrektywy. Zgodnie z art. 23 ust. 1 pkt 4 i 5 UODO przetwarzanie danych jest dopuszczalne tylko wtedy, gdy:

„4) jest niezbędne do wykonania określonych prawem zadań realizowanych dla dobra publicznego,

5) jest to niezbędne dla wypełnienia prawnie usprawiedliwionych celów realizowanych przez administratorów danych albo odbiorców danych, a przetwarzanie nie narusza praw i wolności osoby, której dane dotyczą."

takich jak obecnie możliwości wymiany informacji. Informacja umieszczona w sieci była dotychczas dostępna dla innych pod warunkiem, że wiedzieli, gdzie jej szukać. Pojawienie się nowoczesnych wyszukiwarek i serwisów społecznościowych zniwelowało wszelkie bariery dostępności.

Najistotniejsze znaczenie ma jednak fakt, że usunięcie umieszczonej informacji z jednego źródła nie daje gwarancji, że nie pojawi się ona w innym miejscu. Możliwość zapoznania się z nią, „ściągnięcia" na urządzenie końcowe użytkownika lub utrwalenia w inny sposób, a następnie podzielenia się nią z nieograniczoną liczbą innych użytkowników sprawia, że informacja taka faktycznie pozostanie w obrocie pomimo usunięcia jej z pierwotnego źródła.

Zupełnie odrębną kwestią jest techniczny aspekt „usunięcia" informacji: czy jest to faktyczne usunięcie, czy tylko uniemożliwienie dostępu do niej innym osobom. Wiadomo skądinąd, że informacja „usunięta" z serwisu najczęściej pozostaje na serwerze i istnieje możliwość jej odtworzenia. W słynnej już sprawie zdjęcia na portalu Nasza-klasa pojawiło się zagadnienie podstaw prawnych przechowywania danych na serwerze (nieudostępnianych publicznie). Sprawa – przypomnijmy – ma już drugą odsłonę. Naczelny Sąd Administracyjny w wyroku z 18 listopada 2009 r. (OSK 667/09) potwierdził, że wizerunek osoby jest informacją osobową. Administrator serwisu zaprzestał upubliczniania wizerunku, jednakże kwestionowane zdjęcie pozostało na serwerze, a podstawą prawną – uznaną zresztą przez GIODO – miała być dopuszczalność przechowywania danych w związku z ewentualnymi roszczeniami oraz koniecznością ustalenia odpowiedzialności za naruszenie regulaminu serwisu. Kwestia ta jest obecnie przedmiotem ponownego sporu. Wojewódzki Sąd Administracyjny wyrokiem z 1 grudnia 2010 r. (II SA/Wa 1212/10) uznał przechowywanie danych na serwerze dla powyższych celów za pozbawione podstaw. Wprawdzie nie do końca mogę się zgodzić z niektórymi tezami uzasadnienia[4], niemniej trzeba przyznać, że WSA wyrokiem tym uczynił poważny krok w kierunku urzeczywistnienia prawa do bycia zapomnianym[5].

Nie zmienia to jednak faktu, że w czasie, gdy zdjęcie było dostępne na stronie, każdy mógł je ściągnąć na swój komputer i w dowolnym momencie ponownie umieścić w innym miejscu w sieci. Zawsze więc istnieć już będzie ryzyko, że dane osobowe umieszczone w sieci (w szczególności dane umieszczane w serwisach społecznościowych) będą dostępne dla każdego, kto ma dostęp do globalnej sieci i *de facto* przez nieograniczony czas.

III.

Jak wspomniałem, komunikat Komisji Europejskiej z 4.11.2010 przywołuje używane już w niektórych opracowaniach pojęcie

4 Szczególne wątpliwości budzi teza, że przesłanka dochodzenia roszczeń „dotyczy sytuacji już istniejącej i pewnej, a więc przypadku, gdy istnieje potrzeba udowodnienia, potrzeba dochodzenia roszczenia z tytułu prowadzonej działalności gospodarczej, nie zaś sytuacji, gdy dane są przetwarzane na wypadek ewentualnego procesu i ewentualnej potrzeby udowodnienia, iż dane osobowe pozyskane bez zgody osoby, której dotyczą, są przetwarzane zgodnie z prawem".

5 W omawianej sprawie Generalny Inspektor Ochrony Danych Osobowych wniósł w dn. 13 stycznia 2011 r. skargę kasacyjną, która nie została jeszcze rozpoznana.

prawa do bycia zapomnianym[6]. Warto w tym kontekście odwołać się do poglądów wskazujących psychologiczny i społeczny aspekt zapominania.

Cechą ludzkiej pamięci jest jej zawodność. Zdarza się, że zżymamy się na luki w pamięci, przeszkadza nam, gdy nie możemy przypomnieć sobie szczegółów jakiegoś wydarzenia.

Wisława Szymborska w wierszu „Dnia 16 maja 1973 roku" pisze: *„Jedna z tych wielu dat,/ które nie mówią mi już nic./ Dokąd w tym dniu chodziłam,/ co robiłam – nie wiem./ Gdyby w pobliżu popełniono zbrodnię/ - nie miałabym alibi."*

Zapominanie ma jednak również pozytywne strony zarówno w relacjach formalnych, jak i nieformalnych. Pomaga ludziom w graniu „ról" społecznych, polepszaniu stosunków międzyludzkich itd. Pamięć o popełnionych czynach, grzechy młodości mogą utrudnić nam zdobycie pracy lub np. zaciągnięcie kredytu. Czymże innym jak nie „zapomnieniem" jest instytucja zatarcia skazania?

Tymczasem zaistnienie informacji w sieci oznacza, że zawodna ludzka pamięć będzie wspomagana zasobami Internetu. Google pamięta o nas więcej niż my sami. Można oczywiście powiedzieć, że podobne obawy mieli twórcy pierwszego ustawodawstwa o ochronie danych osobowych pod koniec lat 70. XX w., kiedy to zaczęto wykorzystywać komputery do celów cywilnych, w tym ewidencji ludności. Oto bezduszna maszyna będzie przechowywać i przetwarzać informacje o całym naszym życiu. Obawy w dużej mierze okazały się bezzasadne, ale w tamtych czasach nie było sieci, a komputer był raczej „ucyfrowioną" kartoteką. Dziś ułatwia również komunikowanie się i wymianę informacji z całym światem. Owa powszechna dostępność danych może stać się ciężarem. Oto administrator niemieckiej wersji Wikipedii nie zgadza się na wykreślenie nazwiska mordercy pomimo upływu okresu zatarcia skazania, wobec czego zatarcie traci swoją funkcję społecznego zapomnienia o winie danej osoby. Oto kariera nauczycielska pewnej Amerykanki załamuje się, gdy władze uniwersytetu odkrywają na MySpace Photo jej zdjęcie w pirackiej czapce z kubkiem w dłoni i podpisem „Pijany pirat". Takich przykładów jest coraz więcej, normą stało się, również w Polsce, sprawdzanie w internecie kandydatów do pracy, były także przypadki dyscyplinarnych zwolnień np. gdy pracownik będący na zwolnieniu lekarskim uczestniczył w imprezie i zostało to uwiecznione na zdjęciach umieszczonych na Facebooku lub Naszej-klasie.

Trafne jest twierdzenie, że staliśmy się tym, co można o nas „wygoogolować", włącznie z naszymi „błędami młodości", coraz częściej ocenia się ludzi na podstawie informacji z sieci.

Powyższe przykłady wskazują przy tym na zróżnicowanie sytuacji, które będzie miało znaczenie w sferze ochrony prawnej. Warto przy tym pamiętać, że dużą część informacji na własny temat umieszczamy sami. Stąd być może najważniejszym czynnikiem w reformie prawnej ochrony będzie położenie nacisku na edukację społeczeństwa. Viktor Mayer-Schönberger zachęca do „cyfrowej abstynencji" („digital

6 W niektórych opracowaniach używa się moim zdaniem mniej poprawnego terminu „prawo do zapomnienia". W anglojęzycznych publikacjach używa się terminu „Right to be forgotten", ale np. we Francji mówi się o „droit à l'oubli" („prawo do zapomnienia").

abstinence")[7]. Co jednak zrobić z już umieszczonymi w sieci informacjami lub informacjami na nasz temat umieszczanymi bez naszej wiedzy przez inne osoby? Ponadto digitalizacji podlegają np. stare zdjęcia i dokumenty z czasów, w których nikt nie przypuszczał, że mogą być kiedykolwiek rozpowszechnione.

V. Mayer-Schönberger wskazuje nie tylko na zagrożenia prywatności wynikające z „pamięci absolutnej", jaką oferuje nam sieć. Dysponując doskonałą pamięcią, tracimy zdolność do uogólnienia i myślenia abstrakcyjnego, ryzykując pogubienie się w zapamiętanych szczegółach. Pamięć ludzka wspomagana zasobami sieci będzie zatem nie tylko zagrożeniem naszej prywatności, ale również może negatywnie wpłynąć na stosunki społeczne. Dla tytułowego „pamiętliwego" Funesa z opowiadania J. L. Borgesa doskonała pamięć staje się przekleństwem. Takie osoby funkcjonują również w rzeczywistości: Amerykanka Jill Price, która jest jedną z kilku osób na świecie żyjących z tzw. hipermnezją, czyli zdolnością do nieograniczonego odtwarzania utrwalonych śladów przeżyć psychicznych, potwierdza, że zdolność ta nie pozwala jej na wymazanie z pamięci różnych bolesnych przeżyć. Na pytanie, czy zdolność zapamiętywania niemal wszystkich szczegółów jest dla niej darem czy brzemieniem, odpowiada, że i jednym, i drugim. Z jednej strony dużo pięknych wspomnień, z drugiej – szczegóły sytuacji, co do których na całe życie pozostają wątpliwości, czy zachowało się właściwie[8].

Dziś oczywiście nie możemy porównywać zasobów Internetu z pamięcią absolutną, ale przykład powyższy wskazuje, że im więcej informacji na temat osoby stanie się ogólnodostępnymi, tym gorzej wpłynie to na stosunki międzyludzkie.

Co więcej, sama świadomość, że to co robimy jest widoczne (dostępne) dla innych, niewątpliwie wpłynie na nasze zachowanie, ograniczenie swobody, wreszcie na kształtowanie się postaw oportunistycznych, akceptowalnych przez otoczenie. Wzorcem zachowania może stać się np. umieszczanie na portalach społecznościowych tylko takich zdjęć i informacji, które będą „pożądane" przez przyszłego pracodawcę. Już dziś wiele profili na Facebooku traktuje się jako ważny element „*personal brandingu*", czyli kształtowania własnego wizerunku wobec innych.

Często jednak dzielimy się prywatnymi informacjami nieświadomi powyższych konsekwencji lub też świadomie, stawiając swoją prywatność na dalszym planie. Ekstremalnym przykładem jest tu jeden z podejrzanych o udział w zamachu na WTC, który stwierdziwszy, iż jest śledzony przez amerykańskie służby, zaczął umieszczać w sieci wszystkie szczegóły swojego życia (zdjęcia miejsc, w których aktualnie przebywa, potraw, które jadł itp.), mając nadzieję, że inni stracą zainteresowanie jego prywatnością podaną „na talerzu". Można jednak przypuszczać, że nawet ci, którzy ulegli sloganowi założyciela Facebooka, iż prywatność to przeżytek, nie do końca zdają sobie sprawę z konsekwencji nieograniczonego umieszczania informacji na swój temat w sieci.

Z tego powodu na pytanie, czy ustawodawca powinien przeciwdziałać skutkom ludzkiej nieodpowiedzialności, pomimo że działanie osób było i jest w pełni świadome, odpowiedziałbym pozytywnie. Oczywiście drugim powodem jest również wspomniany wcześniej fakt, że wiele informacji pojawia się w sieci wbrew naszej woli i bez naszej wiedzy.

7 Viktor Mayer-Schönberger, *Delete. The virtue of Forgetting in the Digital Age*, Princeton University Press 2009, omówienie: http://www.youtube.com/watch?v=XwxVA0UMwLY

8 M. Rolff, *Przekleństwo pamięci idealnej*, Süddeutsche Zeitung, przedruk: FORUM nr 20/2011, s. 28

Wydaje się zatem celowe rozważenie sformułowania prawa do bycia zapomnianym przynajmniej odnośnie danych umieszczanych w sieci. Warto zatem ocenić obecne uprawnienia jednostki pod tym kątem.

Jak wspomniałem, prawo do zapomnienia miałoby na celu – jak postuluje Komisja - zapewnienie możliwości żądania przez osobę fizyczną usunięcia danych oraz zaprzestania ich przetwarzania, jeżeli przestałyby być potrzebne do zgodnych z prawem celów.

IV.

Przy ocenie skuteczności dotychczasowych środków ochrony prawnej przewidzianych w Dyrektywie 95/46 oraz w ramach formułowania propozycji mających na celu polepszenie ochrony prywatności w kontekście proponowanej koncepcji „prawa do zapomnienia" należy mieć na uwadze następujące kwestie:

i) prawo do zapomnienia powinno przede wszystkim dotyczyć informacji umieszczanych w sieci, można jednak również rozważyć jego zasadność w stosunku do danych przetwarzanych metodami tradycyjnymi;
ii) środki prawne służące kontroli nad danymi osobowymi powinny współgrać z definicją administratora danych. Wprawdzie w opinii 5/2009 w sprawie portali społecznościowych Grupa Robocza powołana na podstawie art. 29 Dyrektywy stwierdziła, że administratorami danych zamieszczanych na tych portalach są administratorzy portali, ale kwestia ta budzi wątpliwości i powinna być jednoznacznie rozstrzygnięta.
iii) w powyższym kontekście należy również rozważyć kwestię podmiotu zobowiązanego do realizacji obowiązku informacyjnego w przypadku, gdy użytkownik serwisu umieszcza w nim dane o innej osobie. Wspomniana opinia 5/2009 sugeruje, aby serwis informował użytkowników o obowiązku uzyskania zgody osoby trzeciej na umieszczenie jej danych (w przypadku takich serwisów jak Nasza-klasa taki wymóg może podważać sens istnienia serwisu).
iv) w przypadku serwisów społecznościowych realizacja prawa do zapomnienia musi się wiązać nie tylko z realizacją celu, ale również cofnięciem zgody lub zgłoszeniem sprzeciwu, który powinien być równoznaczny z realizacją celu;
v) skuteczna prawna ochrona danych w sieci wymaga instrumentów prawnych o szerszym zasięgu niż Unia Europejska, skuteczność wdrożenia środków wyłącznie na poziomie UE byłaby iluzoryczna, chyba że wdrożonoby system monitorowania i blokowania stron umieszczonych na serwisach spoza UE sprzecznych z prawem unijnym (mało prawdopodobne). Nawet uwzględnienie stanowiska Grupy Roboczej powołanej na podstawie art. 29 Dyrektywy zawartego w opinii 1/2008 dotyczącej zagadnień ochrony danych związanych z wyszukiwarkami określającymi bardzo szeroko zakres podmiotowy Dyrektywy może okazać się niewystarczające.

V.

Istniejące rozwiązania prawne zarówno na szczeblu unijnym, jak i krajowym należy uznać za niewystarczające dla zagwarantowania prawa do zapomnienia w powyższym znaczeniu. Komisja zwraca uwagę, że implementacja cytowanych postanowień Dyrektywy, które mogłyby posłużyć realizacji prawa do zapomnienia, jest zróżnicowana w zależności od państwa członkowskiego.

W związku z powyższymi uwagami można sformułować następujące postulaty co do zmian w unijnych przepisach dotyczących ochrony danych osobowych w kontekście prawa do zapomnienia:

(Dokument): Prawo do zapomnienia jest formułowane wyłącznie w odniesieniu do danych zamieszczanych w sieci. Być może zatem Dyrektywa 95/46 nie jest właściwym miejscem do regulacji tego zagadnienia. Nie jest nim jednak również Dyrektywa 2002/58/WE dotycząca przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej, z uwagi na to, że co do zasady dotyczy ona aspektu ochrony prywatności w ramach działalności telekomunikacyjnej, a nie usług społeczeństwa informacyjnego. Należałoby zatem rozważyć stworzenie nowej regulacji odnoszącej się całościowo do ochrony prywatności i danych osobowych w sektorze łączności elektronicznej i usług świadczonych droga elektroniczną, ewentualnie stworzenie odrębnych przepisów odnoszących się do ochrony prywatności w drugim z wymienionych sektorów.

(Odwoływalność zgody): Podmiot danych powinien mieć prawo do odwołania uprzednio udzielonej zgody na umieszczenie jego danych w sieci.

(Dostęp do danych): Za słuszny należy uznać postulat wprowadzenia terminów odpowiedzi na wnioski o dostęp do danych, jak również terminów reakcji na żądanie usunięcia danych przetwarzanych bez podstaw prawnych.

(Prawo sprzeciwu): Powinno obejmować oprócz dotychczasowych uprawnień żądanie usunięcia danych z sieci bez konieczności udowadniania szczególnej sytuacji, w przypadkach określonych w art. 7 lit. e) i f) (art. 23 ust. 1 pkt 4 i 5 UODO). Żądanie powinno być wolne od opłat. Korzystanie z typowego serwisu społecznościowego nie powinno być traktowane jako realizacja umowy (poza podstawowymi danymi identyfikującymi użytkownika).

(Usunięcie danych): Skutkiem sprzeciwu i cofnięcia zgody powinno być bezwzględne usunięcie danych. I tu również powinny zostać określone terminy wykonania tych czynności.

(Rozwiązania techniczne): Należy propagować rozwiązania techniczne wspierające kontrolę nad danymi. Jedną z propozycji jest koncepcja „daty ważności informacji" („expiry date for information"), zgodnie z którą osoba wprowadzająca informację do sieci decydowałaby o tym, jak długo informacja ma tam pozostać. Istniałaby możliwość przedłużenia terminu ważności. Informacja podlegałaby usunięciu, gdyby jednostka nie przedłużyła terminu („forgetting by default"). Uprawnienie takie powinno przysługiwać również osobom, których dane dotyczą, nawet jeśli nie umieściły ich w sieci. Niektóre propozycje wzorowane są na systemie ochrony praw autorskich („Privacy DRM"). Rozwiązania techniczne powinny również w większym stopniu ograniczać dostęp do informacji ze strony osób niebędących użytkownikami danego serwisu. W wielu przypadkach wskazane byłoby również zróżnicowanie poziomów dostępu poszczególnych użytkowników do poszczególnych kategorii danych. Data ważności informacji nie rozwiązałaby oczywiście wszystkich problemów, szczególnie wtedy, gdy informacja nie pochodzi od osoby, której dotyczy lub gdy informacja dotyczy wspólnie wielu osób.

(Edukacja): Rozwiązania prawne powinny wymuszać edukację internautów, w szczególności co do skutków braku dbałości o prywatne informacje. Ważne byłoby również kształtowanie postaw nastawionych na „information ecology", „digital abstinence" itp.

Podsumowując, należy wskazać, że rozwiązania prawne mogą się okazać zupełnie nieskuteczne, jeśli nie zostaną wsparte rozwiązaniami o charakterze technicznym, a także odpowiednimi działaniami o charakterze edukacyjnym.

Arwid Mednis jest adiunktem na Wydziale Prawa i Administracji Uniwersytetu Warszawskiego oraz wspólnikiem w Kancelarii Wierzbowski Eversheds w Warszawie.

Podpis elektroniczny – prawo i rzeczywistość

Robert Poznański, Daniel Wachnik

Technologia podpisu elektronicznego

Podpisem odręcznym opatrujemy praktycznie każdy dokument w kontaktach z administracją publiczną, a także wiele dokumentów przekazywanych pomiędzy stronami w życiu codziennym. Jest to nie tylko forma potwierdzenia jego autentyczności, ale także wyrażenie zgody i udowodnienia wielu innych atrybutów. Papierowa forma dokumentu zapewnia jego integralność poprzez możliwość podpisania każdej strony, a zawarta na nim data potwierdza czas jego utworzenia. Otrzymując tak przygotowany dokument, możemy także być pewni, że osoba, która się pod nim podpisuje, zapoznała się z jego treścią i wyraziła zgodę na postanowienia w nim zawarte. Za weryfikację autentyczności złożonego podpisu może w szczególności posłużyć wzór podpisu zawarty np. w dowodzie tożsamości osoby.

Wyżej opisane mechanizmy bardzo dobrze sprawdzały się przez długi czas. Jednak dzisiaj coraz popularniejsze staje się wykorzystanie Internetu i poczty elektronicznej do komunikacji między ludźmi, administracją publiczną i różnymi instytucjami komercyjnymi. Wymusza to nowe podejście do stosowanych do tej pory metod uwierzytelnienia i potwierdzenia autentyczności. Możemy sobie przecież wyobrazić sytuację, w której osoba starająca dopuścić się oszustwa skanuje dokument i następnie przy użyciu prostych narzędzi kopiuje obrazek zawierający nasz podpis i wkleja go na inny dokument. Bardzo często po wydrukowaniu takiego dokumentu nie jesteśmy w stanie odróżnić na pierwszy rzut oka, czy taki podpis został skopiowany, czy był napisany odręcznie. Co więcej, w przypadku gdy nie posiadamy papierowego oryginału taki skan jest jedynym śladem, jaki po nim pozostał. Takie rozwiązanie nie daje żadnego bezpieczeństwa i jest bardzo podatne na fałszerstwo.

Naturalną koleją rzeczy było więc wprowadzenie innych metod uwierzytelniania i bardziej zaawansowanych technik dostosowanych do świata Internetu. Nadrzędnym celem było jednak stworzenie systemu bezpiecznego i odpornego na różnego rodzaju ataki. Stało się to możliwe dzięki zastosowaniu dwóch podstawowych metod znanych kryptologii od dłuższego czasu.

Pierwszą z nich jest funkcja skrótu, a drugą kryptografia asymetryczna. Działanie funkcji skrótu polega na wygenerowaniu z dowolnego pliku ciągu bitów, przy czym zmiana nawet jednego bitu w pliku wejściowym powoduje zmianę przynajmniej połowy bitów skrótu. W przypadku podpisu elektronicznego stosuje się funkcję skrótu SHA-1. W najbliższym czasie zostanie ona zastąpiona przez rodzinę SHA-2. Najistotniejszą cechą, która wpływa na bezpieczeństwo tych funkcji, jest długość skrótu, jaki mogą wygenerować. W przypadku SHA-1 jest to 160 bitów, natomiast dla SHA-2 możliwe jest utworzenie skrótu o długości do 512 bitów. Te właściwości powodują, że praktycznie niemożliwe jest utworzenie dwóch różnych zestawów danych mających taki sam skrót. Zastosowanie funkcji skrótu zapewnia integralność dokumentu. Najdrobniejsza nawet zmiana w dokumencie, taka jak dodanie czy usunięcie spacji w dowolnym miejscu, powoduje zmianę jego funkcji skrótu. Jeśli funkcja skrótu dla oryginalnego dokumentu zostanie zapamiętana, można wykryć dowolną zmianę w nim wykonaną.

Mając już dokument zabezpieczony funkcją skrótu, w jaki sposób jesteśmy w stanie udowodnić, że to konkretna osoba opatrzyła go podpisem? W tym celu potrzebujemy narzędzia, którego użyć będzie mogła tylko ona. Tutaj przychodzi nam z pomocą kryptografia asymetryczna. W podpisie elektronicznym najpopularniejszym algorytmem jest RSA (nazwa powstała od złożenia nazwisk twórców: Rivest, Shamir, Adleman). Jego działanie oparte jest na dwóch matematycznie powiązanych ze sobą liczbach zwanymi kluczem prywatnym i kluczem publicznym. Informacje zaszyfrowane przy użyciu klucza prywatnego mogą być rozszyfrowane przy użyciu klucza publicznego i odwrotnie - kluczem publicznym możemy zaszyfrować, a prywatnym odszyfrować. W celu podpisania dokumentu wykorzystywany jest pierwszy przypadek, czyli szyfrowanie kluczem prywatnym i deszyfracja kluczem publicznym. Klucz prywatny jest znany tylko jego właścicielowi, a klucz publiczny jest udostępniany każdemu, kto będzie chciał sprawdzić (odszyfrować) wiadomości przekazane przez właściciela klucza prywatnego. Jeśli odszyfrowanie się powiedzie, można stwierdzić, że dokument został na pewno zaszyfrowany przez osobę, której klucz publiczny został wykorzystany do deszyfrowania. Zaszyfrowaną wiadomość można nazwać podpisem elektronicznym i jest on dołączany do dokumentu.

Jednak posiadanie narzędzi nie zapewni nam jeszcze całkowitej pewności, kto jest autorem dokumentu, ponieważ konieczne jest jeszcze zidentyfikowanie, kto jest posiadaczem klucza publicznego służącego do weryfikacji podpisu Można to robić poprzez osobiste przekazywanie takiego klucza. Jest to jednak uciążliwe, dlatego klucz taki potwierdzany jest jednokrotnie przez organizację powszechnego zaufania - centrum certyfikacji. Wydaje ono elektroniczne potwierdzenia (certyfikaty) zawierające klucz publiczny użytkownika i potwierdzające jego tożsamość. Tożsamość każdej osoby jest weryfikowana podczas procesu wydawania certyfikatu. Dla zapewnienia pełni bezpieczeństwa klucz prywatny generowany jest na karcie kryptograficznej i nigdy jej nie opuszcza. Na takiej karcie zapisywany jest także certyfikat. Karta kryptograficzna wraz z oprogramowaniem służącym do składania i weryfikacji podpisu elektronicznego stanowi w pełni funkcjonalny zestaw.

Na naszym rynku działa pięć firm oferujących zestawy do składania bezpiecznego podpisu elektronicznego. Są to Krajowa Izba Rozliczeniowa SA (Szafir), Unizeto Technologies SA (Certum), Polska Wytwórnia Papierów Wartościowych SA (Sigillum), MobiTrust sp. z o.o. (MobiCert) oraz Enigma SOI sp. z o.o. (CenCert). W skład takiego zestawu wchodzą: czytnik kart kryptograficznych, karta kryptograficzna oraz zapisany na karcie certyfikat, który zawiera parę kluczy RSA, a także informacje o osobie, na którą jest wystawiony. Przy wystawianiu i wydawaniu certyfikatu weryfikowana jest tożsamość osoby. Dostarczane jest także odpowiednie oprogramowanie służące do składania oraz weryfikacji podpisów elektronicznych.

Warto zaznaczyć, iż taka konstrukcja systemu powoduje, że dane służące do składania bezpiecznego podpisu faktycznie znajdują się pod wyłączną kontrolą podpisującego. Certyfikat z parą kluczy znajdują się na karcie kryptograficznej i dostęp do nich chroniony jest kodem PIN. Niemożliwe jest także skopiowanie lub usunięcie kluczy z karty. W specyficznym przypadku, po kilkukrotnym błędnym wpisaniu kodów PIN oraz PUK dostęp do certyfikatu oraz kluczy zostanie zablokowany.

Nowe inicjatywy prawne

Pojęcie podpisu elektronicznego definiuje ustawa o podpisie elektronicznym z dnia 18 września 2001 roku. Podpisem elektronicznym są 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. Jest to definicja bardzo ogólna. Jednak na jej podstawie funkcjonuje tak zwany podpis niekwalifikowany.

W polskim prawie istnieje także pojęcie bezpiecznego podpisu elektronicznego weryfikowanego certyfikatem kwalifikowanym, który spełnia dodatkowe trzy warunki:

1. jest przyporządkowany wyłącznie do osoby składającej ten podpis,
2. jest sporządzony za pomocą podlegających wyłącznej kontroli osoby składającej podpis elektroniczny bezpiecznych urządzeń do składania podpisu elektronicznego i danych służących do składania podpisu elektronicznego,
3. jest powiązany z danymi, do których został dołączony w taki sposób, że jakakolwiek późniejsza zmiana tych danych jest rozpoznawalna.

Aktualnie trwają prace nad dwoma projektami prawnymi dotyczącymi podpisu elektronicznego. Pierwszym jest nowelizacja obecnie obowiązującego rozporządzenia w sprawie warunków technicznych i organizacyjnych dla kwalifikowanych podmiotów świadczących usługi certyfikacyjne, polityk certyfikacji dla kwalifikowanych certyfikatów wydawanych przez te podmioty oraz warunków technicznych dla bezpiecznych urządzeń służących do składania i weryfikacji podpisu elektronicznego. Jej nowelizacja ma na celu dostosowanie obecnie obowiązujących algorytmów szyfrowych do normy ETSI 102 176 zwanej w skrócie ALGO. Norma ta wskazuje na czasowy zakres stosowania oraz parametry algorytmów kryptograficznych, które mogą być używane w technologii podpisu elektronicznego. Wynika z niej, iż certyfikaty kwalifikowane mogą być wydawane na obecnych zasadach do końca 2010 roku. Ze względu na fakt, że została ona wydana w roku 2007, a na dzień dzisiejszy nie są znane skuteczne ataki na podpis elektroniczny o obecnie stosowanych parametrach, rozporządzenie przesuwa termin zmiany parametrów algorytmów na koniec 2011 roku. Od 1 stycznia 2012 roku długość klucza RSA musi mieć minimum 2048 bitów, obecnie są to 1024 bity. W trakcie prac nad rozporządzeniem rozważane było wprowadzenie algorytmu krzywych eliptycznych na poziomie certyfikatu samopodpisanego wydawanego przez NBP. Istotną z prawnego punktu widzenia nowością, którą proponuje ta nowelizacja, jest sposób odniesienia się do norm i standardów unijnych. Zapisy z tych norm nie są już fragmentarycznie kopiowane do tekstu rozporządzenia, ale wstawione są odwołania do konkretnej normy wraz z zakresem jej obowiązywania.

Bardziej medialnym tematem są prace nad nową ustawą o podpisach elektronicznych. Celem jej wdrożenia jest dostosowanie polskiego prawa do wymogów stawianych w dyrektywie 1999/93/EC oraz norm europejskich. Największą nowością jest wprowadzenie nowych definicji podpisów elektronicznych oraz zmiana niektórych już istniejących definicji:

- podpis elektroniczny – dane w postaci elektronicznej dołączone do innych danych elektronicznych lub z nimi logicznie powiązane i służące jako metoda uwierzytelnienia;
- 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;
- podpis kwalifikowany – zaawansowany podpis elektroniczny, składany przez podpisującego będącego osobą fizyczną za pomocą bezpiecznego urządzenia do składania podpisu elektronicznego, weryfikowany za pomocą certyfikatu kwalifikowanego.

Podpis elektroniczny definiowany przez ustawę nie wymusza stosowania mechanizmów opartych na kryptografii asymetrycznej

i funkcjach skrótu. Za podpis elektroniczny zgodny z ustawą można uznać np. podpis składany pod deklaracją PIT. Informacja o kwocie przychodu za poprzedni rok podatkowy wprowadzona do formularza jest „daną w postaci elektronicznej dołączoną do innych danych elektronicznych lub z nimi logicznie powiązaną i służącą jako metoda uwierzytelnienia". Kwota ta pozwala zarówno zweryfikować osobę składającą zeznanie (bo zeznania podatkowe nie są zazwyczaj publikowane), jak i spełnia pozostałe warunki definicji.

Definicja podpisu zaawansowanego jest definicją zaczerpniętą wprost z dyrektywy 99/93/EC. Warunki w niej wymienione wskazują bezpośrednio na użycie kryptografii asymetrycznej i funkcji skrótu. Brak tej definicji w obecnej ustawie o podpisie elektronicznym powoduje problemy, ponieważ prawodawstwo unijne (np. decyzja 2011/130/UE w sprawie minimalnych wymagań dotyczących transgranicznego przetwarzania dokumentów podpisanych elektronicznie) wprost odwołuje się do definicji zaawansowanego podpisu elektronicznego.

Kolejną zmianą wprowadzaną w nowej ustawie o podpisach elektronicznych jest pojęcie pieczęci elektronicznej, które nie funkcjonowało wcześniej. Ideą tego rozwiązania jest stworzenie narzędzia dla firm i organizacji, które nie będzie przypisane do konkretnego pracownika, tylko do całej organizacji:

- 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.

Definicja taka wzbudza jednak wiele kontrowersji. Przede wszystkim czerpie ona wiele z podpisu zaawansowanego, ale odrzuca wymóg wyłącznej kontroli. Pieczęć elektroniczna nie będzie także równoznaczna podpisowi kwalifikowanemu. Jednak kilka kwestii zostało niedopowiedzianych. Są to na przykład tak istotne elementy jak brak opisania skutków prawnych czy określenie jaka instytucja będzie mogła takie pieczęci wydawać.

Nowa ustawa o podpisach elektronicznych wprowadza wiele mechanizmów, które nie istniały wcześniej w polskim ustawodawstwie. Zarówno obywatel, jak i administracja publiczna dostają do użytku pełen asortyment różnorodnych mechanizmów. Warto w tym momencie dodać, iż podpis elektroniczny w kontaktach z administracją publiczną nie musi być realizowany wyłącznie przy pomocy mechanizmów proponowanych przez ustawę o podpisach elektronicznych. Przykładem takim jest choćby podpis osobisty.

Ustawa o dowodach osobistych wprowadza nowe pojęcie z zakresu terminologii podpisu elektronicznego. Jest to podpis osobisty:

- podpis osobisty - dane w postaci elektronicznej złożone za pomocą danych służących do składania podpisu osobistego zawartych w ważnym dowodzie osobistym, które:
  a) wraz z innymi danymi, do których zostały dołączone lub z którymi są logicznie powiązane, pozwalają na identyfikację posiadacza dowodu osobistego,
  b) są przyporządkowane wyłącznie do posiadacza dowodu osobistego,
  c) są powiązane z danymi, do których się odnoszą, w taki sposób, że każda późniejsza zmiana tych danych jest wykrywalna,
  d) są uzupełnione przez ministra właściwego do spraw wewnętrznych danymi pozwalającymi na określenie czasu złożenia tego podpisu.

Co ciekawe, artykuł 3 ustawy o dowodach osobistych mówi, iż „do podpisu osobistego uregulowanego w niniejszej ustawie nie stosuje się przepisów ustawy z dnia 18 września 2001 r. o podpisie elektronicznym". Dodatkowo punkt d) oraz §20 rozporządzenia w sprawie wymagań technicznych dla warstwy elektronicznej dowodu

osobistego oraz protokołu komunikacji elektronicznej z dowodami osobistymi narzucają wymóg dokonania procesu finalizacji podpisu osobistego. Finalizacja może być rozumiana dwojako. W pierwszym przypadku jest jednym z kroków wykonywanych w czasie składania podpisu z mediatorem. Drugą koncepcją realizacji finalizacji może być dodanie przez trzecią stronę, w tym przypadku MSWiA, znacznika czasu. Jednak podstawowym problemem podpisu osobistego jest oderwanie go od ustawy o podpisach elektronicznych. Takie rozwiązanie może spowodować trudności, a nawet uniemożliwić przetwarzanie transgraniczne i interoperacyjność. Byłoby to szczególnie prawdopodobne w przypadku zastosowania technologii podpisu z mediatorem. Dodatkowym problemem są koszty, jakie musiałoby ponieść Ministerstwo Spraw Wewnętrznych i Administracji na zbudowanie centrum certyfikacji pozwalające na finalizację podpisu oraz centra rejestracji użytkowników.

Projekt ustawy o zmianie ustawy o dowodach osobistych, który został opublikowany na stronie BIP MSWiA w dniu 12.04.2011, zakłada likwidację zapisów ustawy, które sugerują zastosowanie podpisu z finalizacją. Po likwidacji wymienionych zapisów podpis osobisty staje się równoważny podpisowi zaawansowanemu. W dalszym ciągu jednak zapisów ustawy o podpisie elektronicznym nie stosuje się do podpisu osobistego.

Nowe technologie i rozwiązania podpisu elektronicznego

Prace dotyczące podpisu elektronicznego toczą się nie tylko na polu prawnym. Instytut Maszyn Matematycznych wraz z firmami Hitachi oraz Mobile Experts prowadzi prace nad rozwojem biometrycznego podpisu elektronicznego skierowanego przede wszystkim do użytku w sferze administracji publicznej. W dobie coraz powszechniejszego wykorzystania biometrii w systemach bankowych oraz bezpieczeństwie zastosowanie tej technologii wydaje się być interesującym rozwiązaniem. Głównym założeniem powyższego projektu jest uwolnienie użytkownika od posiadania karty kryptograficznej i stworzenie infrastruktury pozwalającej na złożenie podpisu elektronicznego w dowolnym miejscu. Żeby taki cel osiągnąć, należy przechowywać klucze prywatne w specjalnie zabezpieczonej bazie danych, podobnie jak wzorce biometryczne każdego użytkownika. Przy pomocy technologii Finger Vein (odczyt wzoru naczyń krwionośnych) każda osoba zarejestrowana w systemie będzie mogła uwierzytelnić się do usługi podpisu elektronicznego. Wszystkie operacje, poza wyliczeniem skrótu dokumentu, wykonywane są na serwerze, a rezultatem ich działań jest podpisany plik. Może on zostać odesłany od razu do właściwego urzędu lub skopiowany np. na pendrive użytkownika. Technologicznie taki podpis nie będzie się niczym różnił od tradycyjnego podpisu złożonego przy użyciu karty kryptograficznej.

Są jednak dwa istotne problemy związane z wykorzystaniem takiego rozwiązania. Pierwszym są obawy przed przechowywaniem cech biometrycznych oraz kluczy prywatnych w centralnej bazie danych. Ich bezpieczeństwo zależeć będzie od sposobu zabezpieczeń oraz uczciwości instytucji, która sprawuje nad nimi kontrolę. Drugą niedogodnością jest cena zaufanych czytników biometrycznych. Może ona okazać się na tyle wysoka, że technologia ta nie przyjmie się w domowych zastosowaniach. Specjalne terminale pozwalające na skorzystanie z systemu musiałyby być instalowane w miejscach użyteczności publicznej jak banki, urzędy pocztowe czy w budynkach administracji publicznej. Istnieje także problem z mocą prawną takiego podpisu. Podpis biometryczny nie zapewnia bowiem wyłącznej kontroli nad danymi służącymi oraz urządzeniem do składania podpisów. Z tego względu, w myśl obowiązujących teraz przepisów, nie będzie to podpis kwalifikowany.

Drugą rozwijającą się prężnie technologią jest tak zwany podpis z mediatorem. Jest to stosunkowo nowe rozwiązanie, opracowywane przez Politechnikę Wrocławską oraz firmę Trustet Information Consulting. Polega ono na stworzeniu

trzeciej strony, zwanej finalizatorem, która bierze aktywny udział w procesie składania podpisu elektronicznego. Jest to technicznie możliwe dzięki podzieleniu klucza prywatnego na dwie części. Jedna zapisana jest na karcie kryptograficznej, na której generowany jest prepodpis. Dopiero finalizator przy użyciu prepodpisu oraz swojej części klucza prywatnego użytkownika jest w stanie wygenerować właściwy podpis elektroniczny.

Zaletą tego rozwiązania jest możliwość sprawdzenia ważności certyfikatu przez trzecią stronę. Jeśli certyfikat jest nieważny, to nie dojdzie do finalizacji. Pozwala to na skrócenie procesu weryfikacji, gdyż istnienie podpisu jest równoznaczne z ważnością certyfikatu. Dodatkowo finalizator może przechowywać logi z działalności użytkownika czy skróty plików, które zostały podpisane. Zasadniczą wadą tego rozwiązania jest brak standaryzacji. Pomimo że istnieje dokumentacja wypracowana przez twórców, nie ma norm europejskich opisujących choćby proces generowania podzielonego klucza prywatnego, procedur jego przesłania do zaufanej trzeciej strony i innych istotnych elementów systemu. Konsekwencją tego jest brak interoperacyjności z innymi projektami eID oraz podpisem elektronicznym implementowanym w krajach Unii Europejskiej.

Podsumowanie

Podpis elektroniczny jest dziedziną podlegającą ciągłym zmianom. W Unii Europejskiej także trwają prace nad nowelizacją dyrektywy 1999/93/EC o podpisach elektronicznych. Głównym ich celem ma być poprawienie transgranicznego uznawania i interoperacyjności podpisów elektronicznych. Nie oznacza to jednak, że nie mogą istnieć rozwiązania na poziomie poszczególnych krajów członkowskich. Prawdopodobnie po zakończeniu prac w Komisji Europejskiej czekają nas kolejne zmiany w polskim prawie. Choć zapewne nie nastąpi to bardzo szybko, gdyż nowa ustawa o podpisach elektronicznych jest już tworzona od kilku lat i w dalszym ciągu nie została wprowadzona w życie. Zmianą, która nas czeka w najbliższym czasie, jest nowelizacja obowiązującego rozporządzenia do ustawy o podpisach. Ma ono wejść w życie w najbliższym czasie, a dostosowanie obecnej infrastruktury do zawartych w nim przepisów ma potrwać do końca 2012 roku. Istotną kwestią, która może wpłynąć na rynek podpisu elektronicznego, jest status podpisu elektronicznego w dowodzie osobistym. Proponowanych rozwiązań jest kilka i w gruncie rzeczy każde z nich ma swoje wady i zalety. Jednak upowszechnienie się podpisu elektronicznego nie zależy wbrew pozorom od wszelkich ustaw, rozporządzeń i zmian, jakie one wprowadzają. Podpis elektroniczny może być traktowany jako drzwi do usług administracji publicznej. Pamiętajmy o budowie domu (usług), bo inaczej po wprowadzeniu elektronicznego dowodu pozostaniemy z 30 milionami drzwi, które stoją w szczerym polu.

Abstract

Electronic signature – law and reality

In this paper we specify legal status of electronic signature in Poland. At the beginning the background of electronic signature is specified, particularly the technology and development of cryptographic technology. There is also described polish market and certification authorities. In the second part of the document development of new act of law and regulations concerning electronic signature are showed. This includes specification of advanced electronic signature, electronic seal and other. Third part describes new technologies like mediated signature and use of biometry in electronic signature with their pros and cons.

Robert Poznański - Specjalista ds. Podpisu Elektronicznego, Instytut Maszyn Matematycznych, Laboratorium Podpisu Elektronicznego i Biometrii.

Daniel Wachnik - Specjalista ds. Podpisu Elektronicznego, Instytut Maszyn Matematycznych, Laboratorium Podpisu Elektronicznego i Biometrii.

Przetwarzanie przez organizację pożytku publicznego danych osobowych osób, które przekazały za pośrednictwem organów skarbowych 1% podatku

Jan Byrski

Wskazanie podstawy legalizującej przetwarzania danych osobowych należy – w świetle przepisów ustawy o ochronie danych osobowych i przepisów szczególnych odnoszących się do przetwarzania danych – do jednego z kluczowych zagadnień prawnych związanych z ochroną danych osobowych zarówno od strony praktycznego podejścia, jak i teoretycznej refleksji. Zasadne wydaje się więc przeanalizowanie, jakie czynności związane z przetwarzaniem danych osobowych podjąć mogą organizacje pożytku publicznego otrzymujące od naczelnika urzędu skarbowego dane osobowe podatnika, po wyrażeniu przez podatnika w zeznaniu podatkowym lub korekcie zeznania zgody na ich przekazanie. Problematyka ta nie doczekała się szerszego zainteresowania doktryny prawa, a wyjaśnienia Generalnego Inspektora Ochrony Danych Osobowych należy uznać za zbyt lakoniczne. Niezbędne wydaje się więc doprecyzowanie tych zagadnień, jak i przedstawienie pozostałych obowiązków nałożonych na organizacje pożytku publicznego, związanych z przetwarzaniem danych osobowych podatników przekazujących 1% podatku na ich rzecz.

Zgoda w ustawie o podatku dochodowym od osób fizycznych

Przekazywanie organizacji pożytku publicznego (zwanej dalej „OPP") danych osobowych osób, które przekazały 1% podatku dochodowego na rzecz konkretnego OPP (zwanych dalej „Darczyńcy"), następuje na podstawie art. 45c ust. 5 ustawy z dnia 26 lipca 1991 r. o podatku dochodowym od osób fizycznych.[1] Przepis ten stanowi, że naczelnik urzędu skarbowego przekazuje dane identyfikacyjne Darczyńców – w tym obojga małżonków w przypadku wspólnego opodatkowania – takie jak imię, nazwisko i adres oraz wysokość przekazanej kwoty, jeżeli podatnik (w rozumieniu podatnik i małżonek w przypadku wspólnego rozliczenia) w zeznaniu lub korekcie zeznania wyraził na to zgodę. W przypadku wskazania przez Darczyńcę celu szczegółowego informacja o takim celu jest również przekazywana organizacji pożytku publicznego.

Rozporządzenie Ministra Finansów z dnia 28 listopada 2008 r. w sprawie określenia wzorów rocznego obliczenia podatku oraz zeznań podatkowych obowiązujących w zakresie podatku dochodowego od osób fizycznych[2], określając wzór deklaracji podatkowej, przewiduje do wypełnienia 3 pola: cel szczegółowy (poz. 126 formularza PIT-37 lub odpowiednik w innych formularzach), miejsce na wyrażenie zgody (poz. 127 lub odpowiednik w innych formularzach) oraz pole na wpisanie dodatkowych informacji, np. ułatwiających kontakt z podatnikiem telefonu czy e-maila (poz. 128 lub odpowiednik w innych formularzach).

Ustawa ani Rozporządzenie nie wskazują celów przetwarzania danych osobowych podatników, w tym celów ich udostępnienia (przekazania) przez

1 Ustawa z dnia 26 lipca 1991 r. o podatku dochodowym od osób fizycznych (tekst jedn. Dz. U. z 2000 r. Nr 14, poz. 176, z późn. zm.), zwana dalej „ustawą o PIT" lub „Ustawą".

2 Rozporządzenie Ministra Finansów z dnia 28 listopada 2008 r. w sprawie określenia wzorów rocznego obliczenia podatku oraz zeznań podatkowych obowiązujących w zakresie podatku dochodowego od osób fizycznych (Dz. U. Nr 212, poz. 1335).

naczelnika urzędu skarbowego do OPP. W istocie zatem jedynym „określonym" przez prawo celem zbierania danych osobowych podatnika – w tym zakresie (kategoriach) – przez naczelnika urzędu skarbowego jest samo ich przekazanie OPP.

Generalny Inspektor Ochrony Danych Osobowych[3] zajął stanowisko, że z wyrażenia zgody na przekazanie danych przez naczelnika urzędu skarbowego do OPP nie można domniemywać, że zgoda obejmuje jakiekolwiek cele przetwarzania danych.[4] Generalny Inspektor wskazał, iż: „*jednocześnie w poz. 128 formularza PIT 37 zawarte zostało określenie ‚cel szczegółowy 1%', jednakże odnosi się to do możliwości dobrowolnego podania przez podatnika celu, na jaki ma zostać wykorzystany przez organizację pożytku publicznego przekazany 1% podatku (...) jakkolwiek zgoda wyrażana przez podatnika dotyczy przekazania dotyczących go danych przez naczelnika urzędu skarbowego organizacji pożytku publicznego, to jednocześnie z treści „cel szczegółowy 1%" nie można domniemywać celów przetwarzania tych danych przez organizację pożytku publicznego*".

Należy mieć wątpliwości – wbrew stanowisku GIODO – czy zgoda taka ma w ogóle charakter „zgody osoby, której dane dotyczą" (art. 7 pkt 5 u.o.d.o.) – oświadczenia woli w rozumieniu ustawy o ochronie danych osobowych[5] (Naczelny Sąd Administracyjny w wyroku z dnia 4 kwietnia 2003 r.,[6] wyraźnie podkreślił, że *„zgoda musi mieć charakter wyraźny, a jej wszystkie aspekty muszą być jasne dla podpisującego w momencie jej wyrażania*" – w tym cel przetwarzania), czy jedynie *quasi*-oświadczeniem procesowym w postępowaniu skarbowym. Udostępnienie danych osobowych przez naczelnika urzędu skarbowego na rzecz OPP następuje *de facto* nie na podstawie zgody podmiotu, którego dane dotyczą, ale na podstawie przepisu prawa – art. 45c ust. 5 ustawy o PIT w związku z „wyrażoną zgodą". Kwestia prawnego charakteru takiej zgody jest jednak wtórna wobec faktu, że w żadnym przypadku zgoda nie może stanowić przesłanki dla przetwarzania danych osobowych przez OPP, innego niż samo ich przechowywanie (archiwizowanie).

Inne podstawy przetwarzania danych osobowych podatników przez OPP

Wypada jednak wskazać, że w Stanowisku GIODO pominął całkowicie istnienie innych przesłanek legalizujących przetwarzanie danych osobowych wskazanych w art. 23 ust. 1 u.o.d.o., a w szczególności przesłanki prawnie usprawiedliwionego celu, o którym mowa w art. 23 ust. 1 pkt 5 u.o.d.o. Zarówno w literaturze,[7] jak i w orzecznictwie[8] *communis opinio* przyjmuje się, że każda z wymienionych w art. 23 ust. 1 u.o.d.o. podstaw

3 Generalny Inspektor Ochrony Danych Osobowych będzie zwany dalej w niniejszym opracowaniu „Generalnym Inspektorem" lub „GIODO".

4 Pismo GIODO z dnia 27 sierpnia 2009 r. (sygn. DOLiS-035-1293/09/31199) skierowane do Pani Urszuli Krasnodębskiej–Maciuły, Prezes Stowarzyszenia Klon/Jawor, ul. Szpitalna 5/5 III p., 00-031 Warszawa, dostępne na stronie internetowej pod adresem elektronicznym: http://wiadomosci.ngo.pl/wiadomosci/583518.html [21.05.2011], zwane dalej „Stanowiskiem GIODO".

5 Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jedn. Dz. U. z 2002 r. Nr 101, poz. 926, z późn. zm.), zwana dalej „u.o.d.o.".

6 Wyrok NSA z dnia 4 kwietnia 2003 r., II SA 2135/02, niepubl.

7 J. Barta, P. Fajgielski, R. Markiewicz, *Ochrona danych osobowych. Komentarz*, Kraków 2007, s. 472-473; J. Byrski, *Odwołanie zgody na przetwarzanie danych osobowych. Wybrane zagadnienia*, Dodatek Specjalny do Monitora Prawniczego 3/2011, s. 17.

8 Wyrok WSA w Warszawie z 1.12.2005, II SA/Wa 917/05, niepubl.; wyrok WSA w Warszawie z 31.03.2006, II SA/WA 2395/04, niepubl.

legalizujących przetwarzanie danych osobowych ma charakter niezależny i autonomiczny, i że są one równoprawne.[9] Określone operacje na danych osobowych administrator danych może wykonywać w oparciu o więcej niż jedną przesłankę, co jest prawnie dozwolone, z zastrzeżeniem sytuacji, że po wygaśnięciu jednej z przesłanek administrator danych może powoływać się na drugą, z uwzględnieniem możliwości odmiennego uregulowania zakresu (kategorii) danych, których przetwarzanie jest dopuszczone na podstawie drugiej przesłanki.

Zgodnie z art. 23 ust. 1 pkt 5 u.o.d.o. dozwolone jest przetwarzanie danych osobowych, jeżeli jest to niezbędne dla wypełnienia prawnie usprawiedliwionych celów realizowanych przez administratorów danych albo odbiorców danych, a przetwarzanie nie narusza praw i wolności osoby, której dane dotyczą. Jak wskazano w art. 23 ust. 4 pkt 1 u.o.d.o., pod pojęciem prawnie usprawiedliwionego celu administratora danych należy rozumieć w szczególności marketing bezpośredni własnych produktów lub usług administratora danych. Należy więc uznać, że OPP posiadają prawną przesłankę legalizującą przetwarzanie danych podatników w tym celu. Skoro w analizowanej sprawie otrzymanie informacji o Darczyńcy pozostaje w jego gestii – wyraża on przecież „zgodę" – trudno mówić o naruszeniu jego praw i wolności w przypadku przetwarzania tychże danych w celach marketingu bezpośredniego (np. wysłania kartki z podziękowaniami za przekazanie 1% podatku).

W tym kontekście istotne jest jedynie określenie, czy przetwarzanie w takim celu danych osobowych – nie tylko ich przechowywanie (archiwizowanie) – nie będzie niezgodne z art. 26 ust. 1 pkt 2 u.o.d.o. Zgodnie z tym przepisem administrator danych zobowiązany jest zapewnić, aby dane osobowe były zbierane dla oznaczonych, zgodnych z prawem celów i niepoddawane dalszemu przetwarzaniu niezgodnemu z tymi celami. Administrator danych (OPP) ich jednak nie zbiera, nie może zatem poinformować o celu zbierania danych. Samo udostępnienie (przekazanie) danych osobowych następuje na podstawie przepisu prawa jedynie w związku z „udzieloną zgodą". W konsekwencji OPP może przetwarzać otrzymane od organów skarbowych – z zachowaniem zasady celowości – dane osobowe:

1. na podstawie wyjątku określonego w art. 26 ust. 2 u.o.d.o., tj. w celach badań naukowych, dydaktycznych, historycznych lub statystycznych, jeżeli nie narusza to praw i wolności osób, których dane dotyczą, z zachowaniem art. 23 (administrator dysponuje przesłanką legalizującą ich przetwarzanie) i art. 25 (wypełniony obowiązek informacyjny albo zwolnienie z niego);
2. w innych celach, jeżeli będą to prawnie usprawiedliwione cele w rozumieniu art. 23 ust. 1 pkt 5 u.o.d.o., w przypadku wypełnienia obowiązku informacyjnego.

Należy również wskazać, że także GIODO trafnie przyjmuje, iż: *„cel przetwarzania można zmienić również wówczas, gdy administrator spełni jeden z warunków wymienionych w art. 23 ustawy oraz wypełni obowiązek informacyjny określony w art. 25 ustawy"*.[10] Stanowisko to powinno znaleźć odpowiednie zastosowanie w przedmiotowym przypadku. Oznaczać to będzie, że OPP będzie mogła wykorzystywać dane osobowe w celach marketingowych na podstawie przesłanki prawnie usprawiedliwionego celu, w przypadku gdy wypełni obowiązek informacyjny wobec takich osób, informując o tym celu (por. poniższe uwagi).

9 Również Generalny Inspektor w Stanowisku wskazuje na taki charakter art. 23 ust. 1 u.o.d.o., jednakże nie analizując w dalszej części innych przesłanek.

10 *GIODO. ABC Ochrony Danych Osobowych*, Wydawnictwo Sejmowe, Warszawa 2007, s. 3.

Obowiązek informacyjny

W przypadku otrzymanych danych osobowych Darczyńców zastosowanie powinien znaleźć art. 25 ust. 1 u.o.d.o., zgodnie z którym administrator danych, w przypadku zbierania danych nie od osoby, której dane dotyczą, zobowiązany jest poinformować ją o:

1. adresie swojej siedziby i pełnej nazwie, a w przypadku gdy administratorem danych jest osoba fizyczna, o miejscu swojego zamieszkania oraz imieniu i nazwisku,
2. celu i zakresie zbierania danych, a w szczególności o odbiorcach lub kategoriach odbiorców danych,
3. źródle danych,
4. prawie dostępu do treści swoich danych oraz ich poprawiania,
5. uprawnieniach wniesienia pisemnego, umotywowanego żądania zaprzestania przetwarzania jej danych ze względu na jej szczególną sytuację oraz możliwości wniesienia sprzeciwu wobec przetwarzania danych w celach marketingowych lub ich udostępniania.

W tym miejscu konieczne jest jednak rozdzielenie dwóch sytuacji:

1. w której OPP będzie jedynie otrzymywała i przechowywała (archiwizowała) dane osobowe Darczyńców oraz
2. gdy OPP będzie w inny sposób (w innym celu) przetwarzała te dane osobowe.

W pierwszym przypadku OPP będą zwolnione z obowiązku informacyjnego na podstawie wyjątku z art. 25 ust. 2 pkt 5 u.o.d.o., tj. dotyczącego przetwarzania danych osobowych na podstawie przepisów prawa przez administratora danych, który jest podmiotem niepublicznym realizującym zadania publiczne. Zgodnie z art. 3 ustawy z dnia 24 kwietnia 2003 r. o działalności pożytku publicznego i o wolontariacie:[11] „*działalnością pożytku publicznego jest działalność społecznie użyteczna, prowadzona przez organizacje pozarządowe w sferze zadań publicznych określonych w ustawie*." Należy zatem uznać, że OPP w zakresie realizacji działań pożytku publicznego stanowią podmioty niepubliczne realizujące zadania publiczne, o których mowa w wyjątku z art. 25 ust. 2 pkt 5 u.o.d.o. Dodatkowo, jak wskazano powyżej, przetwarzanie danych w celu samego przechowywania danych osobowych o Darczyńcach następuje na podstawie przepisu prawa, tj. art. 45c ust. 5 ustawy o PIT.

W drugim przypadku, gdyby dane Darczyńców były przetwarzane w jakimkolwiek innym celu, zwolnienie to nie znajdzie zastosowania. Przetwarzanie danych osobowych nie będzie następowało w oparciu o przepis prawa i nie znajdzie do niego zastosowania art. 25 ust. 2 pkt 5 u.o.d.o. OPP może być wówczas zwolniona z obowiązku informacyjnego jedynie na podstawie art. 25 ust. 2 pkt 3 u.o.d.o., tj. gdy dane są niezbędne do badań naukowych, dydaktycznych, historycznych, statystycznych lub badania opinii publicznej, a ich przetwarzanie nie narusza praw lub wolności osoby, której dane dotyczą, w sytuacji gdy spełnienie obowiązku informacyjnego wymagałoby nadmiernych nakładów lub zagrażałoby realizacji celu badania.

Gdyby OPP zamierzała przetwarzać dane osobowe na podstawie przesłanki prawnie usprawiedliwionego celu (w szeroko pojętych celach marketingowych, jednakże z wyłączeniem tzw. marketingu elektronicznego, do którego niezbędna jest oddzielna zgoda na przesyłanie informacji

11 Ustawa z dnia 24 kwietnia 2003 r. o działalności pożytku publicznego i o wolontariacie (tekst jedn. Dz. U. z 2010 r. Nr 234, poz. 1536, z późn. zm.), zwana dalej „Ustawa o OPP".

handlowej środkami komunikacji elektronicznej[12]), zawsze niezbędna byłaby realizacja obowiązku informacyjnego. Należy zaznaczyć, że obowiązek taki może zostać zrealizowany wraz z pierwszą korespondencją o charakterze marketingowym (np. z podziękowaniami) – jednak w każdym przypadku powinien być zrealizowany niezwłocznie po utrwaleniu (otrzymaniu) przez OPP danych osobowych od naczelnika urzędu skarbowego.

Obowiązek rejestracyjny

Na podstawie art. 40 u.o.d.o. każdy zbiór danych podlega rejestracji. Wyjątki od tej zasady uregulowane są w art. 43 ust. 1 u.o.d.o. Z wyjątków, które teoretycznie mogłyby znaleźć zastosowanie do OPP, należy wskazać zbiory danych przetwarzane:

a) wyłącznie w celu wystawienia faktury, rachunku lub prowadzenia sprawozdawczości finansowej (art. 43 ust. 1 pkt 8 u.o.d.o.),
b) w zakresie drobnych bieżących spraw życia codziennego (art. 43 ust. 1 pkt 11 u.o.d.o.).

Przyjęcie, że zbiory danych Darczyńców podlegają powyższym wyjątkom, jest trudne do zaakceptowania, z zastrzeżeniem gdyby taki zbiór danych był faktycznie przetwarzany wyłącznie na potrzeby sprawozdawczości finansowej.[13] Raczej wykluczona jest kwalifikacja danych osobowych podatków jako danych przetwarzanych w zakresie drobnych bieżących spraw życia codziennego. Do zbiorów takich zaliczane są zbiory pomocnicze (np. przepustek, wejść/wyjść), zbiór zawierający dane osobowe Darczyńców z pewnością nie ma takiego charakteru.

Należy uznać, że co do zasady konieczna jest zatem rejestracja takich zbiorów danych Darczyńców przez OPP. Może nastąpić to albo poprzez rejestrację nowego zbioru danych, albo poprzez „włączenie" tych danych osobowych do już posiadanego i zarejestrowanego zbioru danych. W przypadku gdyby w wyniku „włączenia" zmienił się zakres (kategorie) przetwarzanych danych osobowych, niezbędne będzie złożenie w ciągu 30 dni wniosku aktualizującego, zgodnie z art. 41 ust. 2 u.o.d.o.

Sankcje prawne

W przypadku przetwarzania danych osobowych Darczyńców w szeroko pojętych celach marketingowych (np. zachęcanie do składania darowizn na cel społeczny lub do przekazania także w przyszłym roku 1% podatku na rzecz konkretnego OPP) kluczowe jest wykonanie obowiązku informacyjnego oraz obowiązku zgłoszenia do rejestracji zbioru danych przez OPP. Naruszenie tych obowiązków jest bowiem przestępstwem odpowiednio z art. 54 i art. 53 u.o.d.o. W przypadku spełnienia tych dwóch obowiązków OPP, przetwarzając dane osobowe w celach marketingowych, ryzykuje jedynie ewentualnym wydaniem przez GIODO decyzji zakazującej takiego działania na przyszłość na podstawie art. 18 u.o.d.o. (do czego moim zdaniem nie ma podstaw prawnych).[14] Do momentu wydania decyzji takie działanie nie niesie ryzyka odpowiedzialności karnej, gdyż art. 50 u.o.d.o., penalizujący przetwarzanie danych niezgodnie z celem ich zbierania, został wskutek ostatniej nowelizacji u.o.d.o. uchylony.

12 Zob. art. 9 i 10 ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną oraz X. Konarski, *Komentarz do ustawy o świadczeniu usług drogą elektroniczną*, Warszawa 2004, s. 107-120.

13 Tak też Generalny Inspektor na stronie internetowej pod adresem elektronicznym http://www.giodo.gov.pl/1520049/id_art/2897/j/pl/ [24.05.2011].

14 Generalny Inspektor odpowiadając na pytanie: „*Czy zbiory danych osobowych osób, które wpłaciły 1% podatku na rzecz organizacji pożytku publicznego, zobowiązane są do zgłoszenia do rejestracji Generalnemu Inspektorowi Danych Osobowych?*" wskazał, że „*Jeśli jednak zgromadzone dane służą także innym celom (np. wysyłaniu podziękowań, utrzymywaniu kontaktów z darczyńcami), to administrator (organizacja pożytku publicznego) jest zobowiązany zgłosić przedmiotowy zbiór do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych*." Przesądził tym samym, jak się wydaje, o możliwości prawnej przetwarzania danych osobowych podatników przez OPP w tych celach – http://www.giodo.gov.pl/1520049/id_art/2897/j/pl/ [24.05.2011].

Ewentualna odpowiedzialność z tego tytułu na podstawie art. 49 u.o.d.o. niesie daleko idące wątpliwości prawne.

Podsumowanie

Przetwarzanie danych osobowych Darczyńców przez OPP jest możliwe w celach badań naukowych, dydaktycznych, historycznych lub statystycznych, w przypadku gdy spełnienie obowiązku informacyjnego wymagałoby nadmiernych nakładów, bez wypełnienia tegoż obowiązku informacyjnego. Dopuszczalne jest również przetwarzanie tych danych osobowych w innych prawnie usprawiedliwionych celach administratora danych (OPP), w tym w celach marketingu bezpośredniego, o ile OPP zrealizuje bezpośrednio po utrwaleniu danych obowiązek informacyjny, w tym poinformuje podmiot danych o prawie do wyrażenia sprzeciwu wobec przetwarzania danych w celach marketingowych.

W przypadku jedynie przechowywania otrzymanych od naczelnika urzędu skarbowego danych osobowych należy przyjąć, że OPP jest zwolniona w ogóle z obowiązku informacyjnego na podstawie art. 25 ust. 2 pkt 5 u.o.d.o.

Należy uznać, że zbiory danych Darczyńców powinny podlegać obowiązkowi zgłoszenia zbioru danych do rejestracji. Zbiór ten może stanowić samodzielny zbiór danych albo zostać włączony do innego już zarejestrowanego zbioru danych dotyczącego darczyńców. W przypadku gdyby zmieniło to strukturę zgłoszonego już zbioru danych do jawnego rejestru prowadzonego przez Generalnego Inspektora, konieczne będzie złożenie wniosku aktualizacyjnego przez OPP w terminie 30 dni od dnia dokonania zmiany w zbiorze danych.

Streszczenie

W związku z otrzymaniem danych osobowych Darczyńców od organów skarbowych organizacja pożytku publicznego powinna – co do zasady – wypełnić obowiązek informacyjny przewidziany w art. 25 ust. 1 u.o.d.o. Przetwarzanie jednak tych danych przez OPP jest możliwe w celach badań naukowych, dydaktycznych, historycznych lub statystycznych, w przypadku gdy spełnienie obowiązku informacyjnego wymagałoby nadmiernych nakładów, bez wypełnienia tego obowiązku. Dopuszczalne jest również przetwarzanie danych osobowych w innych prawnie usprawiedliwionych celach administratora danych, w tym w celach marketingu bezpośredniego, o ile OPP zrealizuje bezpośrednio po utrwaleniu danych obowiązek informacyjny, w tym poinformuje o prawie do wyrażenia sprzeciwu wobec przetwarzania danych w celach marketingowych. W przypadku jedynie przechowywania otrzymanych od naczelnika urzędu skarbowego danych osobowych OPP jest zwolniona w ogóle z obowiązku informacyjnego.

Zbiory danych Darczyńców podlegają obowiązkowi zgłoszenia zbioru danych do rejestru prowadzonego przez GIODO.

Jan Byrski - doktor nauk prawnych, adwokat, wspólnik w Kancelarii Prawnej Traple Konarski Podrecki i Wspólnicy.

Upgrade oprogramowania jako przedmiot zamówienia publicznego. Rozważania na tle zamówień na systemy informacji prawnej

Wojciech Kaliński

Zagadnienia wstępne

Kwestia upgrade'u oprogramowania jako przedmiotu zamówienia na gruncie przepisów ustawy z dnia 29 stycznia 2004 r. Prawo zamówień publicznych (t.j. Dz. U. z 2010 r. Nr 113, poz. 759 z późn. zmianami) jest od dłuższego czasu przedmiotem licznych kontrowersji. Problem jest istotnie zagadnieniem złożonym i często nieprawidłowo bądź nieściśle definiowanym, co powoduje, że pojawiające się wątpliwości nie tylko nie są rozwiązywane, lecz na dodatek jeszcze bardziej komplikowane. Z tego względu niniejsza publikacja stanowi próbę rozwiązania wątpliwości narosłych w tym względzie.

Przed przystąpieniem do szczegółowych rozważań konieczne jest poczynienie trzech zasadniczych zastrzeżeń. Po pierwsze, celem niniejszego artykułu nie jest udzielenie odpowiedzi na pytanie, czy zamówienie uprade'u jest możliwe z trybie zamówienia z wolnej ręki. Wynika to z faktu, że pytanie o wybór właściwego trybu postępowania jest pytaniem wtórnym. Pytanie pierwotne, które będzie przedmiotem dalszych rozważań, dotyczy kwestii, czy wskazanie uprade'u jako przedmiotu zamówienia jest w ogóle dopuszczalne, a jeśli tak, to pod jakimi warunkami. Dopiero w razie pozytywnej odpowiedzi na pierwotne pytanie możliwe jest podjęcie dalszych rozważań, a mianowicie, czy tryb zamówienia z wolnej ręki jest właściwym trybem udzielenia takiego zamówienia, czy też należałoby skorzystać z innych trybów. Po drugie, jakkolwiek trzon analizy opierał się będzie na poglądach i orzecznictwie prezentujących problemy związane z zakupem systemów informacji prawnej, to wnioski prezentowane dalej będą miały charakter bardziej uniwersalny. W istocie bowiem zamówienia dotyczące systemów informacji prawnej nie różnią się istotnie (przynajmniej z punktu widzenia systemu zamówień publicznych) od aktualizacji innego rodzaju oprogramowania jak chociażby systemy antywirusowe, oprogramowanie bazodanowe, systemowe czy nawet aplikacyjne. Po trzecie, poza zakresem rozważań pozostaną kwestię korzyści w korzystaniu z upgrade'u oprogramowania wynikające z braku konieczności przeszkolenia personelu zamawiającego w zakresie umiejętności korzystania z nowego oprogramowania, czy też z uwagi na niższe koszty upgrade'u w stosunku do zakupu nowego oprogramowania. Kwestie te albo nie mają znaczenia z punktu widzenia przepisów ustawy – Prawo zamówień publicznych, albo też winny znaleźć swoje odzwierciedlenie w ramach kryteriów oceny ofert, jak np. w cenie.

Przegląd orzecznictwa

W kwestii dotyczącej nabycia prawa do upgrade'u oprogramowania pojawiało się kilka rozstrzygnięć Krajowej Izby Odwoławczej dotyczących nabywania systemów informacji prawnej. Poniżej przedstawiam istotę poszczególnych rozstrzygnięć w porządku chronologicznym.

Orzeczenie Nr 1 - w uchwale Krajowej Izby Odwoławczej Urzędu Zamówień Publicznych z dnia 16 stycznia 2008 r. KIO/KU 1/08 Izba przyjęła stanowisko, zgodnie z którym ochrona praw wyłącznych nie może wynikać z wcześniej zawartych umów, w których zamieszczona była klauzula o ochronie tych

praw. Umowna (kontraktowa) ochrona prawa wyłącznego nie uzasadnia zastosowania trybu zamówienia z wolnej ręki na podstawie art. 67 ust. 1 pkt 1 lit. b ustawy - Prawo zamówień publicznych. Powyższa teza nie oddaje jednak istoty zagadnienia w zakresie nas interesującym. Przedmiotowe rozstrzygniecie zapadło po rozpoznaniu przez Izbę zastrzeżeń do zaleceń pokontrolnych wydanych przez Prezesa Urzędu Zamówień Publicznych w wyniku przeprowadzenia kontroli uprzedniej, zgłoszonych przez Zamawiającego - Zakład Ubezpieczeń Społecznych. Kontrola Prezesa obejmowała przedmiot zamówienia w postaci aktualizacji licencji na korzystanie z programu SIP LEX na 3 lata wraz z rozszerzeniem na nowe stanowiska sieciowe, a w jej wyniku Prezes Urzędu zalecił unieważnienie przedmiotowego postępowania na podstawie art. 93 ust. 1 pkt 7 w zw. z art. 146 ust. 1 pkt 6 ustawy pzp. W uzasadnieniu swojego stanowiska Prezes UZP podniósł m.in., że „*aby skorzystać z przesłanki art. 67 ust. 1 pkt 1 lit. b ustawy pzp należy wykazać dodatkowo, że na rynku nie istnieją rozwiązania równoważne tym, objętym prawem autorskim, które odpowiadałoby potrzebom Zamawiającego. W przeciwnym wypadku niemożliwe jest skorzystanie z trybu zamówienia z wolnej ręki, ponieważ prowadziłoby to do nierównego traktowania wykonawców i preferencji na rzecz rozwiązań opatentowanych. Zamawiający musi dowieść, że wykonanie zamówienia przez innego wykonawcę jest niemożliwe nie tylko ze względu na przysługującą danemu podmiotowi ochronę praw wyłącznych, ale również to, iż istnienie praw wyłącznych skutkuje koniecznością udzielania zamówienia temu podmiotowi.*

W zaleceniach pokontrolnych Prezes Urzędu Zamówień Publicznych wskazał, że obecnie prócz firmy ‚W.' Sp. z o.o. na rynku istnieją również inne podmioty oferujące podobne produkty, np. ‚L. N.' i ‚C.'. A zatem nie jest usprawiedliwieniem udzielenie przedmiotowego zamówienia z wolnej ręki w oparciu o jedynie subiektywne przekonanie Zamawiającego, że tylko jeden wykonawca może je zrealizować.

Prezes Urzędu Zamówień Publicznych nie podzielił również argumentu Zamawiającego, że zakup nowego programu i jego aktualizacja pociągnęłaby za sobą dodatkowe koszty. W opinii Prezesa Urzędu Zamówień Publicznych jest to argument o charakterze gospodarczym, do którego w żadnym wypadku nie odnosi się przepis art. 67 ust. 1 pkt 1 lit. b ustawy pzp. Ekonomiczny aspekt przedsięwzięcia powinien zostać zweryfikowany w oparciu o procedury określone w ustawie pzp, oparte na zasadzie konkurencyjności, które są najlepszym sposobem oceny rynku. W związku z powyższym zdaniem Prezesa Urzędu Zamówień Publicznych wyłonienie wykonawcy zamówienia powinno zostać poprzedzone stosowną weryfikacją. Fakt istnienia podmiotu, którego oferta odpowiada wymaganiom Zamawiającego, nie przesądza o tym, że postępowanie konkurencyjne przeprowadzone w przedmiotowej sprawie nie doprowadzi do wyłonienia innego wykonawcy, którego oferta będzie korzystniejsza dla Zamawiającego, a zarazem spełni wszelkie wymogi stawiane przedmiotowemu zamówieniu."

Ponadto w późniejszym stanowisku Prezes Urzędu zaznaczył, że *„zgodnie z art. 29 ust. 2 ustawy pzp Zamawiający nie może opisywać przedmiotu zamówienia w sposób, który mógłby utrudniać uczciwą konkurencję. Do stwierdzenia faktu nieprawidłowości w opisie przedmiotu zamówienia, a tym samym sprzeczności z prawem, wystarczy jedynie zaistnienie możliwości utrudniania uczciwej konkurencji poprzez zastosowanie określonych zapisów w specyfikacji. Zamawiający powinien unikać wszelkich sformułowań lub parametrów, które by wskazywały na konkretny wyrób albo na konkretnego wykonawcę. Nie można mówić o zachowaniu*

zasady uczciwej konkurencji w sytuacji, gdy przedmiot zamówienia określony jest w sposób wskazujący na konkretnego wykonawcę, przy czym produkt ten nie musi być nazwany przez Zamawiającego, wystarczy, że wymogi i parametry dla przedmiotu zamówienia określone są tak, że aby je spełnić, wykonawca musi dostarczyć jeden konkretny produkt. Działanie takie jest niezgodne z art. 7 ust. 1 ustawy pzp nakazującym równe traktowanie wykonawców i zachowanie uczciwej konkurencji.

W ocenie Urzędu Zamówień Publicznych na rynku istnieje kilka równoważnych rozwiązań, mogących zapewnić dostęp Zamawiającemu do systemów informacji prawnej. Zamawiający zaś opisał przedmiot zamówienia w sposób utrudniający uczciwą konkurencję. Wskazanie przez Zamawiającego konkretnego produktu, który zamierza kupić - przy istnieniu na rynku rozwiązań równoważnych, spełniających jego wymagania - stanowi rażące naruszenie zasady zachowania uczciwej konkurencji i równego traktowania wykonawców.

Ponadto w odpowiedzi na zastrzeżenia zwrócono uwagę na specyfikę udzielenia zamówienia, polegającego na zakupie licencji na korzystanie z systemów informacji prawnej (np. LEX firmy ‚W.' Sp. z o.o.). Zdaniem Urzędu Zamówień Publicznych istotna jest okoliczność, że wraz z zakupem licencji na użytkowanie oprogramowania dostarczana jest przez wykonawcę aktualna baza danych. Zakup licencji obejmuje swoim zakresem możliwość korzystania z oprogramowania, a także jego aktualizację w określonych odstępach czasu (np. comiesięcznie lub codzienne aktualizacje on-line). Licencje te udzielane są na określony czas (np. 12 miesięcy), po upływie którego licencja wygasa i dla dalszego korzystania z oprogramowania konieczny jest zakup nowej licencji. W ocenie Urzędu Zamówień Publicznych bez znaczenia dla Zamawiającego pozostaje więc fakt posiadania bazy danych dla oprogramowania określonej firmy."

Wobec wniosków pokontrolnych Prezesa Urzędu Zamawiający - Zakład Ubezpieczeń Społecznych wniósł zastrzeżenia, wskazując w nich m.in., że *„aktualizacja posiadanego już produktu w postaci licencji nie jest tożsama z zakupem aktualnego produktu, a przedmiotem zamówienia jest zakup kolejnych, comiesięcznych aktualizacji do wcześniej już zakupionych baz przepisów prawnych, nie zaś zakup samej ‚bazy danych'. Zamawiający podkreślił, że bezsporne jest, że każdemu właścicielowi systemu przysługują wyłączne prawa autorskie. Wobec tego bazy Lexa nie może bez jego zgody aktualizować np. ‚C.' czy ‚L. N.' i odwrotnie.*

Zdaniem Zamawiającego zakup nowego produktu nie byłby rozwiązaniem równoważnym, gdyż oznaczałby zakup nowych baz i związanych z nimi licencji, co nie było przedmiotem tego postępowania" oraz że *„... zamówienie dotyczy jedynie zakupu kolejnej aktualizacji oraz rozszerzenia liczby stanowisk sieciowych, bez zwiększenia ilości posiadanych baz".*

Rozpatrując powyższą sprawę, Krajowa Izba Odwoławcza podniosła szereg argumentów, z których do najciekawszych i najistotniejszych należy zaliczyć następujące stwierdzenia:

- *„... licencja na korzystanie z systemu informacji prawnej była każdorazowo udzielana na czas określony, tj. na czas zawarcia umowy.*"
- *„... istnieje na rynku polskim co najmniej kilka podmiotów mogących zrealizować zamówienie w zakresie dostarczenia licencji na system informacji prawnej wraz z dostawą baz danych i ich aktualizacją."*

- *„... każdy z systemów informacji prawnej, związana z nim baza danych i ich ewentualna aktualizacja podlegają ochronie prawnej. Nie wyklucza to jednak możliwości realizacji dostarczenia licencji na system informacji prawnej wraz z dostawą baz danych i ich aktualizacją przez inny podmiot. W warunkach konkurencji Zamawiający może wybrać produkt podlegający ochronie prawnej, który w najpełniejszy sposób odpowiadałby jego potrzebom."*
- *„... skorzystanie z wyżej zacytowanej przesłanki, jako podstawy do udzielenia zamówienia z wolnej ręki, jest wykluczone w sytuacji, gdy na rynku istnieją rozwiązania równoważne w stosunku do tych objętych prawem autorskim lub wyłącznym, które są jednocześnie zgodne z wymaganiami Zamawiającego. Ponieważ jak wykazano wyżej, istnieją na rynku rozwiązania równoważne w zakresie dostarczania systemów informacji prawnej spełniające oczekiwania Zamawiającego, nie jest zatem możliwe udzielenie zamówienia jednemu wykonawcy ze względu na ochronę praw wyłącznych."*
- *„Zdaniem Krajowej Izby Odwoławczej udzielenie zamówienia publicznego na aktualizację licencji na korzystanie z programu SIP LEX na 3 lata wraz z rozszerzeniem na nowe stanowiska sieciowe w trybie zamówienia z wolnej ręki z powołaniem się na przesłankę określoną w art. 67 ust. 1 pkt 1 lit. b ustawy pzp, w sytuacji istnienia rozwiązań równoważnych, doprowadziłoby do nierównego traktowania wykonawców i nieuzasadnionych preferencji na rzecz jednego, wskazanego przez Zamawiającego podmiotu."*
- *„Jak wynika z treści postanowień §2 pkt 4 umowy z dnia 25 listopada 2004 roku nr (...), licencje, o których mowa w §2 ust. 1 pkt 1a i b, zostały udzielone na okres od listopada 2004 roku do października 2007 roku. Zatem udzielona tą umową licencja wygasła, a wraz z nią wygasło prawo do korzystania z baz danych. Wobec tego Zakład Ubezpieczeń Społecznych, aby móc dalej korzystać z oprogramowania oferowanego przez ‚W.', musi dokonać zakupu licencji wraz z aktualnymi bazami danych. Zatem aktualizacja, o której mówi Zamawiający, polegać będzie w istocie na zakupie nowych baz danych i ich aktualizacją wraz z licencją do korzystania z nich."*

Orzeczenie nr 2 – w uchwale Krajowej Izby Odwoławczej Urzędu Zamówień Publicznych z dnia 26 września 2008 r. KIO/KU 5/08 Izba zajęła stanowisko, iż przesłanki udzielenia zamówienia z wolnej ręki na podstawie art. 67 ust. 1 pkt 1 lit. a ustawy - Prawo zamówień publicznych muszą mieć charakter jednoznacznie wypływający z uprzednich norm, parametrów i standardów, a ich jednoznaczność nie powinna pozwalać na jakiekolwiek odstępstwa. Sytuacja ta może występować z uwagi na unikatowe, niepowtarzalne cechy uprzednich prac wykonanych w następstwie wcześniejszego zamówienia. Również i ta teza nie tłumaczy istoty zagadnienia związanego z tematem niniejszej publikacji, stąd konieczne jest sięgnięcie do szczegółowych argumentów zawartych w uzasadnieniu przedmiotowego orzeczenia.

Podobnie jak poprzednie orzeczenie analizowana uchwała zapadła w związku z zaleceniami pokontrolnymi wydanymi przez Prezesa Urzędu Zamówień Publicznych wskazującymi na obowiązek unieważnienia postępowania na podstawie art. 93 ust. 1 pkt 7 w zw. z art. 146 ust. 1 pkt 6 pzp w przedmiocie postępowania o udzielenie zamówienia publicznego na: zawarcie trzyletniej umowy licencyjnej dotyczącej aktualizacji 1210 jednostanowiskowych wersji systemu informacji prawnej LEX Omega oraz serwera internetowego systemu informacji prawnej SIP LEX INTRANET, pozwalającego na równoczesną pracę 100 użytkowników w centrali i delegaturach NIK prowadzonego w trybie zamówienia z wolnej ręki - art. 67

ust. 1 pkt 1 lit. a i b pzp. W ocenie Prezesa Urzędu *„przepis art. 67 ust. 1 pkt 1 lit. a znajduje zatem zastosowanie w sytuacji, gdy na rynku, obiektywnie rzecz biorąc, istnieje tylko jeden wykonawca zdolny zrealizować określone zamówienie. Konieczne jest zatem obiektywne ustalenie przez Zamawiającego, czy w danej sytuacji, w odniesieniu do danego konkretnego zamówienia istnieją jacykolwiek inni alternatywni wykonawcy, którzy mogliby potencjalnie zrealizować zamówienie. Wystarczy, że na rynku działa co najmniej dwóch lub większa liczba podmiotów mogących wykonać zamówienie, aby możliwość zastosowania przedmiotowego trybu z przyczyn technicznych była wyłączona*." Prezes UZP również zwrócił uwagę na „*specyfikę udzielenia zamówienia polegającego na zakupie licencji na korzystanie z systemów informacji prawnej. Licencje te bowiem obejmują swoim zakresem możliwość korzystania z oprogramowania, a także jego aktualizację w określonych odstępach czasu (np. comiesięczne lub codzienne aktualizacje on-line). Wraz z zakupem licencji na użytkowanie oprogramowania dostarczana jest przez wykonawcę aktualna baza danych. Licencje te udzielane są na określony czas (np. 12 miesięcy). Po jego upływie licencja wygasa i dla dalszego korzystania z oprogramowania konieczny jest zakup nowej licencji. Bez znaczenia pozostaje więc dla Zamawiającego fakt posiadania bazy danych dla oprogramowania określonej firmy - licencja na korzystanie z tego oprogramowania bowiem wygasła i dla jego dalszej eksploatacji konieczny będzie zakup nowej licencji.”*

W zastrzeżeniach pokontrolnych Zamawiający podniósł m.in., że „*licencje te - wbrew ustaleniom poczynionym przez Prezesa UZP - nie wygasają po zakończeniu obecnie obowiązujących umów (w dniu 28 września 2008 r.), a jedynie wymagają aktualizacji. Po upływie terminu, do którego obowiązują obecnie trwające umowy, Zamawiający będzie miał nadal prawo do korzystania z baz danych (skoro licencje w tym zakresie są bezterminowe), jednak bazy aktów prawnych nie będą aktualizowane o nowe akty (przedmiot umowy, której dotyczą zastrzeżenia, dotyczy właśnie aktualizacji). Nie może być kwestionowane, że aktualizować bazę danych może tylko jej autor.*”

Uwzględniając zastrzeżenia zamawiającego, Krajowa Izba oparła się na dwóch zasadniczych argumentach:

1) na konieczności posiadania przez zamawiającego bazy aktów prawnych własnych oraz
2) na fakcie, że licencje na korzystanie z bazy aktów prawnych posiadane przez Zamawiającego są bezterminowe.

W odniesieniu do pierwszego z argumentów Krajowa Izba Odwoławcza zauważyła, że „*jedynie ‚W.’ sp. z o.o. ma w swojej ofercie możliwość korzystania ze zbioru własnych aktów prawnych, tj. oferuje produkt posiadający istotną dla Zamawiającego właściwość, której nie mają inne produkty dostępne na rynku, oferowane przez podmioty wymienione w zaleceniach pokontrolnych.*”

Jeśli chodzi o argument nr 2, Krajowa Izba stwierdziła m.in., że:

- „*Zamawiający posiada bezterminowe licencje pozwalające na korzystanie z bazy danych, przedmiotem zamówienia z wolnej ręki jest aktualizacja tychże licencji. Nie może budzić wątpliwości, iż tylko właściciel praw autorskich do bazy danych ma prawo bazę danych aktualizować. W ocenie Izby, co do zasady, ‚nabycie praw wyłącznych nie może wynikać z wcześniej zawartych umów, w których zamieszczona była klauzula o ochronie tych praw’ (jak wskazał Prezes UZP w zaleceniach pokontrolnych), jednak bez wątpienia należy dopuścić przypadki, kiedy taka ochrona jest nieunikniona (np. nadzór autorski nad*

realizacją projektu budowlanego). W ocenie Izby taka sytuacja zaistnieje również wówczas, kiedy Zamawiający dysponuje trwającą w czasie licencją na bazę danych, a zamierza nabyć jej aktualizację."

- *„Wydaje się, że w zaleceniach pokontrolnych mylnie utożsamiono licencję na korzystanie z bazy danych/korzystanie z oprogramowania z licencją na jej aktualizację.*"
- *„Aby być uprawnionym do korzystania z bazy danych, konieczna jest licencja. Korzystanie z bazy danych jest (technicznie) możliwe, kiedy dysponuje się odpowiednim oprogramowaniem (również licencjonowanym), które w przypadku systemu informacji prawnej ma charakter akcesoryjny w stosunku do bazy danych - pełni rolę służebną wobec bazy danych. Baza aktów prawnych wraz z oprogramowaniem umożliwiającym korzystanie z niej to ‚system informacji prawnej'. Na podstawie przywołanych wyżej umów łączących Zamawiającego z ‚W.' Sp. z o.o. Izba ustaliła, że posiadane przez Zamawiającego licencje na korzystanie z bazy danych (bazy aktów prawnych) są bezterminowe. Na czas określony udzielane były licencje na aktualizację baz danych (zamówienia z wolnej ręki udzielane przez Prezesa UZP w aktach pokontrolnych). Po wygaśnięciu licencji na aktualizację nie wygasa prawo do korzystania z bazy danych (w zaleceniach pokontrolnych mylnie uznano, że ‚dla jego (oprogramowania) dalszej eksploatacji konieczny będzie zakup nowej licencji'; można z niej korzystać bezterminowo, lecz baza danych nie jest aktualizowana o nowe akty prawne)."*
- *„Oczywiście, można byłoby zbadać, czy wobec istnienia na rynku kilku podmiotów oferujących bazy aktów prawnych nie byłoby celowe (korzystne gospodarczo) zaprzestanie korzystania z posiadanych licencji i zakup nowych (niewykluczone, że od innego podmiotu) wraz z ich aktualizacją w trybie konkurencyjnym; wydaje się, że to właśnie miały na celu zalecenia pokontrolne Prezesa UZP. Jednak, jak uznano w części I uzasadnienia niniejszej uchwały, baza danych oferowana przez ‚W.' Sp. z o.o. jako jedyna posiada możliwość korzystania z bazy aktów prawnych własnych Zamawiającego, zatem uzasadnione jest dalsze korzystanie przez Zamawiającego z posiadanych licencji bezterminowych na korzystanie z bazy aktów prawnych i co za tym idzie - nabycie licencji na ich aktualizację."*

<u>Orzeczenie nr 3</u> – kolejne orzeczenie obejmuje uchwałę Krajowej Izby Odwoławczej Urzędu Zamówień Publicznych z dnia 8 maja 2009 r. KIO/KD 12/09, podjętą podobnie jak dwie poprzednie w następstwie rozpatrzenia zarzutów do zaleceń pokontrolnych Prezesa Urzędu Zamówień Publicznych zgłoszonych przez Agencję Rynku R. w związku z postępowaniem o udzielenie zamówienia publicznego na zakup licencji na System Informacji Prawnej „L." w wersji Intranet plus moduły: Komentarze, IP-G, Prawo Europejskie na okres 1-2 lat, na około 70 stanowisk przeprowadzonym w trybie zamówienia z wolnej ręki - art. 67 ust. 1 pkt 1 lit. b pzp. I podobnie jak w poprzednich postępowaniach Prezes Urzędu podniósł, iż *„dla zastosowania trybu zamówienia z wolnej ręki w oparciu o art. 67 ust. 1 pkt 1 lit. b ustawy Prawo zamówień publicznych konieczne jest bowiem stwierdzenie, że istnieje tylko jeden wykonawca zdolny do zrealizowania zamówienia, ze względu na konieczność ochrony uregulowanych w odrębnych przepisach praw wyłącznych, a zamawiający musi wykazać, że na rynku nie istnieją zgodne z jego wymaganiami rozwiązania równoważne do tych objętych prawem wyłącznym - zatem niezbędne jest wykazanie, że produkty te mogą być wytworzone lub dostarczone tylko przez określonego wykonawcę. W innym wypadku skorzystanie z trybu zamówienia z wolnej ręki prowadziłoby bowiem do nierównego traktowania wykonawców.*

Tymczasem na rynku funkcjonuje kilka podmiotów (tj. ‚L.' Sp. z o.o., C.H. ‚B.' Sp. z o.o., ‚W.' Sp. z o.o., ‚K.' Sp. z o.o.) oferujących odpowiadające zapotrzebowaniu Zamawiającego

programy, które zawierają bazy aktualnych aktów prawa polskiego i wspólnotowego wraz z orzecznictwem. Skoro zatem istnieją podmioty, które są w stanie zrealizować zamówienie w sposób prawidłowy, oferując program równoważny, prawa autorskie do określonego oprogramowania nie stanowią bariery dla udzielenia zamówienia podmiotowi oferującemu inny program, który również zawiera wymagane funkcjonalności."

W zarzutach do wyników kontroli Zamawiający wśród argumentów podniósł m.in., że *„...System Informacji Prawnej ‚L.' zawiera informacje w dużym zakresie niedostępne w innych programach prawniczych ... Zatem pomimo podobieństwa innych programów nie są one w istocie programami równoważnymi i konkurencyjnymi do zakupionego."* Zamawiający dodał także, iż posiada licencje bezterminowe na korzystanie z programu.

Krajowa Izba, popierając stanowisko Zamawiającego, oparła się w istocie na jednym zasadniczym argumencie: *„Jeżeli bowiem uznać za wiarygodny fakt - a brak dowodów przeciwnych - że tylko ‚W.' ma w swojej ofercie możliwość korzystania z wymaganego przez Zamawiającego zbioru aktów prawnych i opracowań, tylko on ma możliwość spełnienia świadczenia pożądanego przez Zamawiającego, a więc zajmuje on pozycję tzw. ‚naturalnego monopolisty'. Potwierdzenie tej okoliczności jest, zdaniem składu orzekającego Izby, kluczowe dla ustalenia, czy istniały podstawy do udzielenia zamówienia z wolnej ręki. Niewątpliwie bowiem w przypadku, kiedy dany produkt jest oferowany tylko przez jednego wykonawcę, istnieją przesłanki do udzielenia zamówienia publicznego na podstawie art. 67 ust. 1 pkt 1 lit. b ustawy Prawo zamówień publicznych*."

Orzeczenie nr 4 – to kolejne rozstrzygnięcie zapadłe w następstwie rozpoznania przez Krajową Izbę Odwoławczą zarzutów wobec wyników kontroli Prezesa Urzędu Zamówień Publicznych w postaci uchwały Krajowej Izby Odwoławczej Urzędu Zamówień Publicznych z dnia 24 czerwca 2010 r. KIO/KD 43/10, w której KIO przedstawiło następujące stanowisko: *„Wobec posiadania przez Zamawiającego bezterminowych licencji na system informacji prawnej ‚L.' nie znalazłoby oparcia w przepisach prawa zobowiązanie Zamawiającego do przeprowadzania postępowania o udzielenie zamówienia publicznego za każdym razem, gdy zakończy się okres subskrypcji. Zobowiązanie takie prowadziłoby do sytuacji, w której Zamawiający zmuszony byłby zakupić ponownie, bez względu na dostawcę, program, którym już de facto dysponuje."*

Powyższe rozstrzygniecie zapadło w następstwie rozpoznania wyników kontroli Prezesa UZP postępowania prowadzonego przez „N." pn.: „Dostęp do systemu informacji prawnej ‚L.' on-line w sieci WAN" udzielonego w trybie zamówienia z wolnej ręki. W zastrzeżeniach pokontrolnych Prezes Urzędu powtórzył praktycznie w całości argumentację przytoczoną powyżej w omówieniu orzeczeń nr 1-3., uzupełniając je następującym wywodem: *„Dla spełnienia dyspozycji ww. przepisu[1] konieczne jest istnienie praw wyłączonych (np. autorskich) oraz jednego podmiotu zdolnego do realizacji przedmiotu zamówienia, a także związek przyczynowo-skutkowy pomiędzy ww. okolicznościami. Ponadto w świetle zasad ogólnych wyrażonych w przepisach Pzp niedopuszczalne jest przyjęcie stanowiska, iż zaistnienie przesłanki do udzielenia zamówienia z wolnej ręki związanej z ochroną praw wyłącznych ma źródło w zdarzeniach, za których zaistnienie odpowiedzialność ponosi Zamawiający,*

1 Art. 67 ust. 1 pkt 1 lit b) pzp – przyp. wł.

*który ukształtował postanowienia pierwotnej umowy dot. korzystania z serwisu ‚L.' w tym zakresie. Przy czym należy wziąć pod uwagę, iż majątkowe prawa autorskie, o których stanowi ustawa z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych (Dz. U. 2006 r. Nr 90 poz. 631 ze zm.) są zbywalne, a dzia*łający z należytą starannością *Zamawiający powinien uwzględnić, iż brak tego typu postanowień umownych może doprowadzić do sytuacji ograniczających konkurencję w rozumieniu ustawy.*"

Zamawiający w zastrzeżeniach do wyników kontroli podniósł „*…istotność specyficznych rozwiązań zawartych jedynie z systemie ‚L.' dla prowadzenia jego statutowej działalności związanej z ochroną zdrowia. Zamawiający porównał funkcjonalności oraz liczbę rekordów w tej dziedzinie oferowane w różnych produktach dostępnych na rynku."*

Krajowa Izba Odwoławcza, rozpatrując przedmiotową sprawę, zastrzegła, iż „*... podstawą rozstrzygnięcia Izby w przedmiocie wyniku niniejszej kontroli jest fakt, że zamawiający posiada system informacji prawnej ‚L.', który w świetle załączonych do przedmiotowych zastrzeżeń wyjaśnień ‚W.' Sp. z o.o., może w wersji niezaktualizowanej bezterminowo użytkować.*

Tym samym ciągłość korzystania z systemu informacji prawnej ‚L.' nie została przerwana, Zamawiający nadal korzysta z baz danych, których aktualizacji zaprzestano. Powyższy fakt ma w ocenie Izby zasadnicze znaczenie dla rozstrzygnięcia niniejszych zastrzeżeń. Izba stwierdziła, że wobec posiadania przez Zamawiającego bezterminowych licencji na system informacji prawnej ‚L.' nie znalazłoby oparcia w przepisach prawa zobowiązanie zamawiającego do przeprowadzania postępowania o udzielenie zamówienia publicznego za każdym razem, gdy zakończy się okres subskrypcji. Zobowiązanie takie prowadziłoby do sytuacji, w której Zamawiający zmuszony byłby zakupić ponownie, bez względu na dostawcę, program, którym już de facto dysponuje" oraz że: „*dodać należy, że nic nie stoi na przeszkodzie, aby Zamawiający w przyszłości, po przeprowadzeniu analizy rynku i stwierdzeniu ewentualnych korzyści z wymiany dotychczasowego oprogramowania, podjął decyzję o zaprzestaniu korzystania z oprogramowania dotychczasowego i o zakupie nowego w trybie konkurencyjnym*."

<u>Orzeczenie nr 5</u> – to Wyrok Krajowej Izby Odwoławczej Urzędu Zamówień Publicznych z dnia 27 kwietnia 2010 r. KIO/UZP 487/10, który zapadł w następującym stanie faktycznym. Zamawiający, tj. Województwo Ł., zamieścił w Biuletynie Zamówień Publicznych ogłoszenie o udzieleniu zamówienia publicznego w trybie z wolnej ręki na przedłużenie abonamentu na System Informacji Prawnej „L." dla Samorządu Terytorialnego wraz z Serwisem HR. Odwołanie wobec czynności Zamawiającego polegającej na wyborze zamówienia z wolnej ręki wniosło Wydawnictwo „B." Sp. z o.o., zarzucając Zamawiającemu naruszenie art. 67 pkt 1 lit. B pzp, podnosząc, że: *„…. sam fakt istnienia praw licencyjnych nie wyklucza możliwości nabycia systemu informacji prawnej od innych wykonawców. Odwołujący zauważył również, że każdy z trzech oferowanych na rynku systemów informacji prawnej posiada zespół cech go wyróżniających. Wskazał, że Zamawiający zobowiązany jest wykazać, że jedynie produkt o określonych przez niego cechach umożliwia mu realizację celu założonego w ramach postępowania. Wskazywanie na określone funkcjonalności zamawianego produktu bez wyraźnego wykazania obiektywnej konieczności takiego opisu przedmiotu zamówienia stanowi, w ocenie Odwołującego, rażące naruszenie prawa, jeśli Zamawiający w ten sposób dokona ograniczenia konkurencji, zawężając krąg potencjalnych wykonawców."*

Krajowa Izba Odwoławcza powołanym wyrokiem oddaliła wniesione odwołanie, powołując się na następującą argumentacje: „*Podstawą rozstrzygnięcia Izby w niniejszej sprawie jest fakt, że Zamawiający posiada system informacji prawnej ‚L.', na który udzielone zostały Zamawiającemu licencje na czas nieokreślony (co jest zgodne z art. 143 ust. 1 pkt 5 ustawy Pzp). Jak wynika z treści Ogólnych Warunków Umowy dot. Korzystania z ‚L.' dla Samorządu Terytorialnego nr (...), użytkownik może korzystać z programu przez czas nieokreślony, przy czym upoważnienie do korzystania z programu obejmuje te wersje, które zostały użytkownikowi dostarczone w okresie abonamentu (pkt 11.1 i 11.2). Tym samym ciągłość korzystania z systemu informacji prawnej ‚L.' nie została przerwana, Zamawiający nadal korzysta z baz danych - po dniu 31 grudnia 2009 r. zaprzestano jedynie aktualizacji programu. Powyższy fakt ma w ocenie Izby zasadnicze znaczenie dla rozstrzygnięcia sprawy. Izba stwierdziła, że wobec posiadania przez Zamawiającego bezterminowych licencji na system informacji prawnej ‚L.' nie znalazłoby oparcia w przepisach prawa zobowiązanie Zamawiającego do przeprowadzania postępowania o udzielenie zamówienia publicznego za każdym razem, gdy zakończy się okres aktualizacji programu. Zobowiązanie takie prowadziłoby do sytuacji, w której Zamawiający zmuszony byłby zakupić ponownie, bez względu na dostawcę, program, którym już de facto dysponuje. W ocenie Izby wymóg prowadzenia odrębnych postępowań w podstawowych trybach zaistniałby w sytuacji, gdyby licencje na korzystanie z programu udzielone zostały na czas określony i możliwość użytkowania oprogramowania wygasałaby wraz z końcem umowy, co jednak nie ma miejsca w przedmiotowym stanie faktycznym*." Dodatkowo Izba zaznaczyła, że „*Izba wzięła pod uwagę fakt, że Odwołujący kwestionuje wybór trybu zamówienia z wolnej ręki, podnosząc zarzuty dotyczące opisu przedmiotu zamówienia, zmierzające do rezygnacji przez Zamawiającego z aktualizacji posiadanego oprogramowania i zakupu nowego systemu informacji prawnej*" oraz „*… że nieuprawnione jest wymaganie od Zamawiającego, aby zmienił przedmiot zamówienia w taki sposób, aby Odwołujący mógł się o nie ubiegać, a przez to ponownie zakupił oprogramowanie, które już posiada.*"

Orzeczenie nr 6 – to wyrok Krajowej Izby Odwoławczej Urzędu Zamówień Publicznych z dnia 30 kwietnia 2010 r. KIO/UZP 577/10, który zapadł w następującym stanie faktycznym. Zamawiający - Narodowy Bank Polski - zamieścił w Biuletynie Zamówień Publicznych ogłoszenie o zamiarze zawarcia umowy w trybie z wolnej ręki na odnowienie subskrypcji baz System Informacji Prawnej ‚L1.' z modułami Komentarze, Prawo Europejskie i Informator Prawno-Gospodarczy. Odwołanie wobec czynności Zamawiającego polegającej na wyborze zamówienia z wolnej ręki wniosła ‚L.' Sp. z o.o., podnosząc argumenty analogiczne do przedstawionych w orzeczeniu nr 5.

Krajowa Izba Odwoławcza, oddalając odwołanie, zauważyła, że „*podstawą rozstrzygnięcia Izby w niniejszej sprawie jest fakt, że Zamawiający posiada system informacji prawnej ‚L1.', na który udzielone zostały Zamawiającemu licencje na czas nieokreślony (pkt 11 Ogólnych Warunków Umowy Nr (...)). Jak wyjaśnił Przystępujący w treści przystąpienia do postępowania odwoławczego i czemu nie zaprzeczył Odwołujący, w przypadku licencji na czas nieokreślony, po zakończeniu umowy Zamawiający może korzystać bezterminowo z ostatniej aktualnej wersji systemu. Tym samym ciągłość korzystania z systemu informacji prawnej ‚L1.' nie została przerwana, Zamawiający nadal korzysta z baz danych - po dniu 14 kwietnia 2010 r. zaprzestano jedynie aktualizacji programu. Powyższy fakt ma w ocenie Izby zasadnicze znaczenie dla rozstrzygnięcia niniejszej sprawy. Izba stwierdziła, że wobec posiadania przez Zamawiającego bezterminowych licencji na system informacji prawnej ‚L1.'*

nie znalazłoby oparcia w przepisach prawa zobowiązanie Zamawiającego do przeprowadzania postępowania o udzielenie zamówienia publicznego za każdym razem, gdy zakończy się okres subskrypcji. Zobowiązanie takie prowadziłoby do sytuacji, w której Zamawiający zmuszony byłby zakupić ponownie, bez względu na dostawcę, program, którym już de facto dysponuje. W ocenie Izby wymóg prowadzenia odrębnych postępowań w podstawowych trybach zaistniałby w sytuacji, gdyby licencje na korzystanie z programu udzielone zostały na czas określony i możliwość użytkowania oprogramowania wygasałaby wraz z końcem umowy, co jednak nie ma miejsca w przedmiotowym stanie faktycznym."

Analiza problematyki

Jakkolwiek, zgodnie z założeniami niniejszej publikacji, jej zakres ma być szerszy niż tylko odniesienie do systemów informacji prawnej, to jednak nim przystąpię do szczegółowej analizy wynikających z powołanych orzeczeń problemów, na wstępie konieczne jest wyjaśnienie wątpliwości dotyczących relacji między prawem do korzystania z programu komputerowego a prawem do korzystania z baz danych, które to zagadnienia zostały dosyć mocno zagmatwane, w szczególności w wywodach z zawartych w orzeczeniu nr 2.

Punktem wyjścia winno być twierdzenie, że system prawa polskiego przewiduje niezależną ochronę utworom w rozumieniu art. 1 ustawy z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych (t.j. Dz. U. z 2006 r. Nr 90 poz. 631, z późn. zmianami), obejmującym także i programy komputerowe oraz odrębny reżim ochronny dla baz danych, określony przepisami ustawy z dnia 27 lipca 2001 r. o ochronie baz danych (Dz. U. Nr 128, poz. 1402, z późn. zmianami). Do nowelizacji obydwu ustaw dokonanej ustawą z dnia 9 maja 2007 r. o zmianie ustawy o prawie autorskim i prawach pokrewnych oraz niektórych innych ustaw (Dz. U. Nr 99, poz. 662)[2] oba systemy ochrony miały charakter rozłączny. Art. 1 ustawy o ochronie baz danych stanowił bowiem, że ochronie określonej w ustawie podlegają bazy danych, z wyłączeniem baz danych spełniających cechy utworu określone w ustawie z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych (Dz. U. z 2000 r. Nr 80, poz. 904). Chcąc zatem ustalić, czy określony system, np. system informacji prawnej, podlega ochronie specyficznej dla baz danych czy ochronie prawno-autorskiej, należało w pierwszej kolejności ustalić, czy system ten ma cechy utworu (w rozumieniu art. 1 ustawy o prawie autorskim), czy też nie. W razie odpowiedzi pozytywnej system chroniony był zgodnie z przepisami autorskimi; w razie odpowiedzi negatywnej reżimem właściwym były przepisy dot. baz danych.

Po wspomnianej nowelizacji przepisów z 2007 r. sytuacja uległa istotnej zmianie. Art. 1 ustawy o ochronie baz danych otrzymał bowiem brzmienie: *„Bazy danych podlegają ochronie określonej w ustawie niezależnie od ochrony przyznanej na podstawie ustawy z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych (Dz. U. z 2006 r. Nr 90, poz. 631, Nr 94, poz. 658, Nr 121, poz. 843 oraz z 2007 r. Nr 99, poz. 662) bazom danych spełniającym cechy utworu."* Oznacza to, że w przypadku gdy baza danych spełnia jednocześnie cechy utworu, podlega równoległej ochronie w reżimie przepisów o ochronie baz danych i przepisów o prawie autorskim i prawach pokrewnych.

Z punktu widzenia przepisów ustawy o ochronie baz danych, w zakresie związanym z tematem niniejszej publikacji, należałoby

2 Nowelizacja weszła w życie 20 czerwca 2007 r.

zwrócić szczególną uwagę na dwie regulacje. Zgodnie z art. 2 ust. 1 pkt 1 ustawy o ochronie baz danych w rozumieniu ustawy baza danych oznacza zbiór danych lub jakichkolwiek innych materiałów i elementów zgromadzonych według określonej systematyki lub metody, indywidualnie dostępnych w jakikolwiek sposób, w tym środkami elektronicznymi, wymagający istotnego, co do jakości lub ilości, nakładu inwestycyjnego w celu sporządzenia, weryfikacji lub prezentacji jego zawartości. Natomiast stosownie do art. 4 tejże ustawy ochrona przyznana bazom danych nie obejmuje programów komputerowych użytych do sporządzenia baz danych lub korzystania z nich.

Dostępne na polskim rynku systemy informacji prawnej to rozwiązania, które składają się – z punktu widzenia prawnego – z dwóch elementów: baz danych (w rozumieniu cytowanego wyżej art. 2 ust. 1 pkt 1) oraz programów komputerowych umożliwiających korzystanie z przedmiotowych baz. Oba te elementy decydują w podobnym stopniu o przydatności danego systemu informacji prawnej dla poszczególnych użytkowników. Dla jednych istotniejsze będzie posiadanie jak największej bazy danych, zawierającej maksymalną liczbę aktów prawnych, ich rodzajów, zbioru orzeczeń itp., co z pewnością jest podstawowym elementem decydującym o kosztach tworzenia danego systemu, dla innych zaś kluczowe znaczenie będą miały mechanizmy wyszukiwania, szybkość działania, wygląd i funkcjonalność interfejsu itp. Niezależnie jednak od preferencji decydujących o wyborze takiego czy innego systemu informacji prawnej, „nabywając" taki system, odbiorca uzyskuje dwojakiego rodzaju uprawnienia licencyjne: po pierwsze licencję[3] na program komputerowy, służący do korzystania z bazy aktów prawnych, orzeczeń i innych elementów dostępnych w bazie; a po drugie licencję[4] na korzystanie z bazy danych. Kwestię tę dobrze ilustruje definicja oprogramowania zastosowana w warunkach licencyjnych DVD LexisNexis Polska Spółka z ograniczoną odpowiedzialnością od dnia 1 lutego 2009 r., zgodnie z którymi to warunkami przez oprogramowanie rozumie się *„... oprogramowanie komputerowe służące do korzystania z publikacji wymienionej w otrzymanej fakturze, w skład którego wchodzą: program instalacyjny, baza danych z zakresu prawa, program komputerowy w formacie kodu obiektowego służący do obsługi bazy danych poprzez wyszukiwanie odpowiednich danych i informacji zawartych w bazie"*.[5] Ten dwoisty system licencjonowania został pośrednio zasygnalizowany w orzeczeniu nr 2 Krajowej Izby Odwoławczej: *„Aby być uprawnionym do korzystania z bazy danych, konieczna jest licencja. Korzystanie z bazy danych jest (technicznie) możliwe, kiedy dysponuje się odpowiednim oprogramowaniem (również licencjonowanym), które w przypadku systemu informacji prawnej ma charakter akcesoryjny w stosunku do bazy danych - pełni rolę służebną wobec bazy danych. Baza aktów prawnych wraz z oprogramowaniem umożliwiającym korzystanie z niej to ‚system informacji prawnej'",* jakkolwiek bez dokładniejsze analizy teoretyczno prawnej. Co ciekawe, w późniejszych orzeczeniach Krajowej Izby Odwoławczej problem dwoistego charakteru systemu informacji prawnej zanika, a kolejne składy KIO wydają się traktować oba elementy systemu jako jedną całość, jak np. w Orzeczeniu nr 6: *„w przypadku licencji na czas nieokreślony, po zakończeniu umowy Zamawiający może korzystać bezterminowo z ostatniej aktualnej wersji systemu. Tym samym ciągłość korzystania z systemu informacji prawnej ‚L1.' nie została przerwana, Zamawiający nadal korzysta z baz danych - po dniu 14 kwietnia 2010 r. zaprzestano*

3 W rozumieniu przepisów ustawy i prawie autorskim i prawach pokrewnych.
4 W rozumieniu przepisów ustawy o ochronie baz danych.
5 Warunki licencji DVD od dnia 1 lutego 2009 r. – dostępne w wersji elektronicznej w programie LexPolonica Perfecta firmy LexisNexis Polska Spółka z ograniczoną odpowiedzialnością.

jedynie aktualizacji programu. Powyższy fakt ma w ocenie Izby zasadnicze znaczenie dla rozstrzygnięcia niniejszej sprawy. Izba stwierdziła, że wobec posiadania przez Zamawiającego bezterminowych licencji na system informacji prawnej ‚LI.' nie znalazłoby oparcia w przepisach prawa zobowiązanie Zamawiającego do przeprowadzania postępowania o udzielenie zamówienia publicznego za każdym razem, gdy zakończy się okres subskrypcji." To wielka szkoda, albowiem zarówno Krajowa Izba Odwoławcza, jak i Prezes Urzędu Zamówień Publicznych nie dostrzegli niezwykle istotnego problemu prawnego, jaki pojawia się w związku z tym w przypadku licencjonowania systemów informacji prawnej w systemie zamówień publicznych. Otóż zgodnie z art. 143 ust. 1 pkt 5 pzp na czas nieoznaczony może być zawierana umowa, której przedmiotem są dostawy licencji na oprogramowanie komputerowe. Przepis ten dopuszcza zatem zawierania umów licencyjnych na czas nieokreślony, ale tylko w odniesieniu do programów komputerowych. Możliwości takiej nie ma w odniesieniu do licencji na korzystanie z baz danych, które podlegają ograniczeniom wynikającym z art. 142 ust 2 pzp (mogą być zawierane tylko na czas oznaczony). Tym samym nie do końca prawdziwe są twierdzenia zawarte w cytowanych orzeczeniach Krajowej Izby Odwoławczej, zgodnie z którymi Zamawiający mają prawo do bezterminowych licencji na korzystanie z systemu informacji prawnej w wersji nieaktualizowanej. Ponieważ, jak wspomniano, system informacji prawnej składa się z programu komputerowego i bazy danych, powyższe zdanie jest prawdziwe jedynie w odniesieniu do programu komputerowego. Natomiast zapisy umów licencyjnych w zakresie odnoszącym się do niepodlegającej aktualizacji bazy danych są sprzeczne z art. 142 ust. 2 pzp, co oznacza, że licencja na korzystanie z samej niepodlegającej aktualizacji bazy danych jest udzielana na czas oznaczony[6], a nie nieoznaczony. To niewątpliwa luka w rozumowaniu Krajowej Izby Odwoławczej prezentowanym w przedstawionych wyżej wyrokach. Luka, które jednak nie musi przesądzać, że końcowe wnioski zawarte w tych orzeczeniach są błędne.

Należy zauważyć, że z analogiczną konstrukcją prawną będziemy mieli do czynienia w przypadku oprogramowania komputerowego korzystającego z różnorodnych baz danych. Dotyczy to w szczególności oprogramowania antywirusowego, systemów typu firewall itp., w przypadku których korzystanie z bazy danych i samego programu komputerowego jest równie istotne.

Streszczenie

Publikacja przedstawia problematykę sposobu licencjonowania systemów informacji prawnej typu Lex z uwzględnieniem licencji na program komputerowy służący do korzystania z bazy aktów prawnych, orzeczeń i innych elementów dostępnych w bazie oraz licencję na korzystanie z bazy danych na gruncie orzeczeń KIO oraz przenosi zagadnienia prawne powstające na tym tle na szerszy grunt kwestii dopuszczalności opisu przedmiotu zamówienia jako upgrade'u rozwiązania informatycznego już istniejącego u danego Zamawiającego i związanego z tym ograniczenia konkurencji.

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

6 Nie wchodząc w szczegółowe rozważania dotyczące czasu korzystania z takiej nieaktualizowanej bazy, wydaje się, że licencja taka udzielana jest na cztery lata zgodnie z art. 142 ust. 2 pzp. Natomiast z uwagi na brak podstaw do stosowania analogi nie wydaje się zasadnym odpowiednie korzystanie do baz danych z regulacji art. 66 ustawy o prawie autorskim i prawach pokrewnych.

Biuletyny Informacji Publicznej sądów i prokuratur w województwie śląskim – raport z badania

Grzegorz Wójkowski

W marcu br. Stowarzyszenie Bona Fides z Katowic opublikowało raport „Biuletyny Informacji Publicznej sądów i prokuratur w województwie śląskim”[1], który jest wynikiem monitoringu przeprowadzonego w okresie od marca do czerwca oraz w grudniu 2010 roku w sądach i prokuraturach województwa śląskiego.

Badanie zostało przeprowadzone w ramach projektu „Przejrzysta Temida”, współfinansowanego ze środków Unii Europejskiej w ramach Europejskiego Funduszu Społecznego. Raport został przygotowany wspólnie przez prezesa Stowarzyszenie Bona Fides Grzegorza Wójkowskiego oraz dr Sławomira Tkacza, pracownika naukowego Wydziału Prawa i Administracji Uniwersytetu Śląskiego w Katowicach.

Przedmiotem przeprowadzonego monitoringu było sprawdzenie stron BIP z punktu widzenia ich zawartości i zgodności z wymaganiami prawa, a także ocena ich przejrzystości i funkcjonalności. Należy podkreślić, że podczas monitoringu nie ograniczono się jedynie do dokonania ustaleń w zakresie, czy strony BIP zawierają te informacje, które w świetle przepisów prawa podmioty zobowiązane powinny udostępniać. Zwrócono także uwagę na zagadnienia, których publikacja nie ma charakteru obligatoryjnego, ale są ważne z punktu widzenia interesu indywidualnego i społecznego.

Monitoring realizowany był na podstawie trzech specjalnych narzędzi badawczych. Pierwsze wykorzystane zostało do sprawdzania stron BIP sądu apelacyjnego i sądów okręgowych, drugie – sądów rejonowych, a trzecie - prokuratur. Podczas badania dokonano przeglądu Biuletynów Informacji Publicznej i jedynie w minimalnym zakresie zajmowano się oficjalnymi witrynami internetowymi sądów i prokuratur.

Biuletyny Informacji Publicznej sądów

Podsumowując wyniki monitoringu Biuletynów Informacji Publicznej sądów województwa śląskiego, warto zwrócić uwagę na duże różnice w jakości biuletynów pomiędzy sądami, które prowadzą dwa serwisy internetowe (BIP i strona WWW), a tymi, które prowadzą jeden serwis spełniający wymogi stawiane stronom BIP.

W tym pierwszym przypadku informacje zawarte na stronie BIP są z reguły znacznie bardziej skromne. W wielu przypadkach strony BIP są aktualizowane rzadko bądź niemal w ogóle od lat nie są aktualizowane, większość informacji umieszczana jest natomiast na stronach WWW.

Do tej grupy zaliczyć można stronę Sądu Rejonowego w Dąbrowie Górniczej, gdzie, poza ofertami pracy i zamówieniami publicznymi, w BIP znajduje się dziewięć zakładek, z których siedem nigdy od czasu powstania biuletynu (2007 r.) nie było aktualizowanych. Wynika to głównie z bardzo

1 Raport dostępny jest na stronie www.bonafides.pl.

skąpej zawartości zakładek. Przykładowo: jedyna informacja udostępniona na stronie BIP dotycząca struktury sądu brzmi następująco: *„Jednostkami organizacyjnymi tut. Sądu są Wydziały i Oddziały, których zakres działania jest zgodny z przepisami ustawy Prawo o ustroju sądów powszechnych."*

Jeżeli osoba zainteresowana poszukuje informacji na temat struktury organizacyjnej Sądu Rejonowego w Dąbrowie Górniczej, to musi ona zignorować BIP i przeszukać stronę WWW sądu, gdzie w przejrzysty sposób podane są wszystkie niezbędne informacje łącznie z imionami i nazwiskami kierowników, numerami telefonów, numerami pokojów i godzinami przyjęć interesantów.

Odrębny problem dotyczy Sądu Rejonowego w Sosnowcu, który w ogóle nie prowadzi strony BIP, natomiast posiada rozbudowaną i funkcjonalną stronę internetową. W naszym przekonaniu sformułowane w tej materii wnioski stanowią asumpt na rzecz konieczności podjęcia w praktyce działań, których efektem będzie likwidacja dualizmu oficjalne serwisy internetowe – strony Biuletynu Informacji Publicznej. Niewątpliwie idealnym stanem w tej materii będzie sytuacja, w której każdy zainteresowany będzie mógł odszukać wszelkie potrzebne informacje na jednej stronie internetowej, na której zostaną one udostępnione na mocy przepisów rangi ustawowej.

Innym problemem, na który należy zwrócić uwagę, jest niewywiązywanie się bądź niedostateczne wywiązywanie się sądów z nałożonych przez prawodawcę obowiązków na mocy ustawy o dostępie do informacji publicznej. Dotyczy to w szczególności art. 8 ust.6., w którym mowa jest o odpowiednim oznaczaniu informacji umieszczanych w biuletynie. Przeprowadzony monitoring pozwala na sformułowanie wniosku ogólnego, iż trudno którąkolwiek z badanych stron BIP uznać w tym zakresie za idealną (problemy dotyczą głównie odpowiedniego oznaczenia osoby, która wytworzyła informację lub odpowiada za jej treść oraz z oznaczenia czasu wytworzenia informacji).

Szczególny problem dotyczy strony biuletynu Sądu Okręgowego w Bielsku-Białej, który w ogóle zrezygnował z oznaczania treści udostępnianych w BIP.

Również część informacji, których obowiązek umieszczania w BIP wynika z art. 6 ustawy o dostępie do informacji publicznej, nie jest przez wiele sądów udostępniana w biuletynie. Przykład tego stanowi dokumentacja przebiegu i efektów kontroli, której nie publikuje żaden z badanych sądów. Często na stronach BIP brakuje także innych obowiązkowych informacji (zwłaszcza w przypadku sądów rejonowych), np. dotyczących majątku czy prowadzonych przez sąd rejestrów i ewidencji.

Należy zauważyć, iż zakres informacji udostępnionych na stronach BIP sądu apelacyjnego oraz sądów okręgowych jest z reguły znacznie szerszy w relacji do stron sądów rejonowych. Dla przykładu 34,5% sądów rejonowych podaje informacje na temat kompetencji każdego wydziału, 48,3% dotyczące majątku sądu, 58,6% dotyczące sposobu wniesienia pisma do sądu, a 65,5% podaje numery kont bankowych. W przypadku sądu apelacyjnego i sądów okręgowych wyżej wymienione informacje znajdują się we wszystkich poddanych badaniu biuletynach.

Ostatni problem, który należy podnieść w świetle przeprowadzonych badań, stanowi duża ilość pustych, bardzo skromnych w treść bądź od dawna nieaktualizowanych

zakładek, które można znaleźć w większości biuletynów badanych sądów. W naszym przekonaniu winny zostać podjęte czynności celem usunięcia występujących w tym zakresie nieprawidłowości.

Na zakończenie należy odnotować, iż pomimo tego że przeprowadzony monitoring pozwolił na stwierdzenie zaistnienia pewnych problemów, sformułować należy wniosek ogólny, iż znaczna część monitorowanych biuletynów prowadzona jest w sposób bardzo przejrzysty, a zakres udostępnianych w BIP informacji uznać należy za wystarczający.

Warto także podkreślić, że część sądów publikuje w biuletynach BIP większy zakres informacji od tych, które stanowiły przedmiot przeprowadzonych badań. Dla przykładu: często na stronach BIP umieszcza się broszury informacyjne „Prawa i obowiązki obywatela w sądzie i prokuraturze". Praktykę w tej materii należy ocenić zdecydowanie pozytywne. Godna naśladowania jest także praktyka Sądu Rejonowego w Katowicach, który udostępnia wiele dodatkowych informacji, m.in. regulamin korzystania z pokojów gościnnych, informacje na temat przesłuchania na odległość czy informacje dla osób niepełnosprawnych.

Biuletyny Informacji Publicznej prokuratur

Monitorowane biuletyny Prokuratury Apelacyjnej w Katowicach oraz poszczególnych prokuratur okręgowych umieszczone są w formie zakładek na stronie podmiotowej Biuletynu Informacji Publicznej Prokuratury Generalnej. Część stwierdzonych podczas badania nieprawidłowości, dodajmy: które trudno uznać za bardzo liczne, zwłaszcza w części dotyczącej organizacji strony podmiotowej BIP stanowi wynik tego, iż biuletyn Prokuratury Generalnej nie realizuje w pełni wszystkich wymogów wynikających z treści przepisów ustawy o dostępie do informacji publicznej oraz z rozporządzenia Ministra Spraw Wewnętrznych i Administracji w sprawie Biuletynu Informacji Publicznej.

Dotyczy to m.in. modułu wyszukującego, który nie pozwala na ograniczenie wyszukiwania tylko do podstrony określonej prokuratury okręgowej, a także stopki z danymi, która w każdym przypadku odnosi się do całej podstrony, nawet w sytuacji, gdy umieszczonych jest na niej kilka niezależnych informacji publicznych.

W świetle wyników monitoringu można sformułować wniosek ogólny, iż wszystkie poddane badaniom prokuratury udostępniają informacje dotyczące sposobu przyjmowania i załatwiania spraw. Stopień ich szczegółowości i przydatności dla zainteresowanych, a także przejrzystości, w poszczególnych jednostkach nie jest natomiast jednakowy.

Na stronach BIP badanych podmiotów niewiele jest jednakże informacji, które w formie poradnika mogą służyć uczestnikom oraz stronom postępowania. W szczególności, żadna z monitorowanych prokuratur nie publikuje w BIP informacji dotyczącej praw i obowiązków pokrzywdzonego, podejrzanego oraz świadka.

Powyższe informacje nie zostały także udostępnione na stronie BIP Prokuratury Generalnej, natomiast udostępniono na niej zakładkę, w której można pobrać szereg ustaw oraz aktów wykonawczych (brak jednakże przykładowo k.p.k.).

W praktyce osoby zainteresowane mogą uzyskać o wiele więcej informacji w tym zakresie na stronach internetowych poszczególnych prokuratur. Strony BIP poszczególnych jednostek nie

zawierają jednakże, wbrew przepisom aktu wykonawczego, czytelnych linków do istniejących serwisów informacyjnych każdej z nich.

Mając na uwadze to, że biuletyny wszystkich prokuratur są zakładkami na stronie podmiotowej BIP Prokuratury Generalnej, wydaje się, iż należy sformułować postulat, aby właśnie w tym miejscu zamieścić przejrzyście opracowany poradnik dla stron oraz uczestników postępowania, z którego mogłyby korzystać osoby z całej Polski zainteresowane informacjami w zakresie swoich praw i obowiązków oraz procedur związanych z funkcjonowaniem prokuratury.

Przeprowadzony monitoring musi także prowadzić do postawienia pytania, czy można ocenić jako wystarczającą współpracę pomiędzy administratorem strony BIP Prokuratury Generalnej i administratorami BIP pozostałych prokuratur.

Z jednej strony w biuletynie Prokuratury Generalnej znajduje się zakładka „akty prawne", w której, jak stwierdzono powyżej, w czytelny sposób zamieszczone zostały do pobrania teksty ustaw i rozporządzeń regulujących funkcjonowanie prokuratury. Na stronach BIP jednostek organizacyjnych podległych Prokuraturze Generalnej brak jest natomiast linków, które odsyłałyby do tych aktów.

Z drugiej natomiast strony każda z poddanych badaniom prokuratur w swoim BIP wskazuje akty prawne stanowiące podstawy ich działalności, jednakże brak jednolitości w tej materii; w jednym przypadku stwierdzono nawet powołanie aktu, który utracił moc obowiązującą.

Wydaje się, iż w tej sytuacji postulować należy umieszczenie aktów prawnych stanowiących podstawy prawne działalności poszczególnych jednostek organizacyjnych tylko w jednej zakładce znajdującej się na stronie BIP Prokuratury Generalnej, do której odsyłałyby linki z biuletynów prokuratur podległych. Jasne jest bowiem to, iż akty prawne stanowiące podstawę prawną działalności prokuratur w przypadku każdej z nich są tożsame.

Kończąc omawianie Biuletynu Informacji Publicznej Prokuratury Generalnej, warto jeszcze zwrócić uwagę na brytyjską flagę, która umieszczona jest u góry strony, sugerującą, że biuletyn posiada także wersję w języku angielskim. Niestety, jak wynika z zamieszczonej metryczki, już od ponad roku jedyną informacją, która pojawia się po kliknięciu na flagę, jest napis „Under construction...".

Wracając do biuletynów monitorowanych prokuratur z terenu woj. śląskiego, badanie wykazało, że na ich stronach BIP nie ma określonych informacji, których publikowanie stanowi ustawowy obowiązek. Przykładem tej praktyki są informacje o naborze kandydatów na wolne stanowiska pracy, które w biuletynie umieszczają jedynie dwie z pięciu badanych prokuratur. Dotyczy to także konkursów na stanowisko asystenta prokuratura czy też naborów na staż urzędniczy, choć w świetle przepisów ustawowych nie budzi wątpliwości to, iż informacje w tej materii powinny być ogłaszane w BIP.

Konkludując, stwierdzić należy, iż w monitorowanych Biuletynach Informacji Publicznej prokuratur woj. śląskiego znajduje się większość wymaganych w świetle obowiązujących przepisów prawa podstawowych informacji dotyczących ich struktury i zasad funkcjonowania. Niewiele jest jednak dodatkowych informacji. Stan ten może jednakże stanowić następstwo

przyjętej konstrukcji tych stron, zgodnie z którą biuletyny wszystkich prokuratur są zakładkami na stronie podmiotowej BIP Prokuratury Generalnej, czego następstwem jest to, iż poszczególne jednostki organizacyjne o wiele więcej informacji ogłaszają na własnych stronach internetowych.

Zaznaczyć trzeba jednakże, iż pomimo tego, że badane biuletyny są zakładkami na stronie Biuletynu Informacji Publicznej Prokuratury Generalnej, różnią się one często pomiędzy sobą nie tylko zawartością merytoryczną, ale także sposobami udostępniania danych. Może to w praktyce utrudnić osobom zainteresowanym dotarcie do informacji publicznych.

Streszczenie

W marcu br. Stowarzyszenie Bona Fides z Katowic opublikowało raport „Biuletyny Informacji Publicznej sądów i prokuratur w województwie śląskim", który jest wynikiem monitoringu przeprowadzonego w sądach i prokuraturach województwa śląskiego. Przedmiotem badania było sprawdzenie stron BIP z punktu widzenia ich zawartości i zgodności z wymaganiami prawa, a także ocena ich przejrzystości i funkcjonalności. Raport został przygotowany wspólnie przez prezesa Stowarzyszenie Bona Fides Grzegorza Wójkowskiego oraz dr Sławomira Tkacza, pracownika naukowego Wydziału Prawa i Administracji Uniwersytetu Śląskiego w Katowicach.

Grzegorz Wójkowski - prezes zarządu i koordynator projektów strażniczych w Stowarzyszeniu Bona Fides.

Zapraszamy do udziału

SEMINARIUM
„ELEKTRONICZNE TWORZENIE I OGŁASZANIE AKTÓW PRAWA MIEJSCOWEGO"
30 sierpnia 2011 r., Warszawa

W PROGRAMIE:
- Internet jako źródło aktów prawnych.
  Piotr Waglowski (Vagla.pl)
- ePUAP jako wygodne narzędzie do elektronicznego przekazywania aktów prawnych.
  dr Zbigniew Olejniczak (CPI MSWiA)
- Zarządzanie elektronicznym zbiorem aktów normatywnych w Urzędzie Miasta Siedlce.
  Marzanna Prekurat (Kierownik Biura Rady Miasta)
- Wdrażanie dyrektywy Re-use.
  Piotr Waglowski (Vagla.pl)
- Nowelizacja ustawy o ogłaszaniu aktów normatywnych - aspekty praktycznego stosowania.
  Ryszard Adam Grytner (konsultant i ekspert w zakresie organizacji i funkcjonowania administracji publicznej, A&BC)
- Internetowy System Informacji Prawnej.
  dr Zbigniew Jabłoński (Kancelaria Sejmu RP)
- Doświadczenia z wydawania w formie elektronicznej Dziennika Ustaw i Monitora Prawnego.
  Jarosław Deminet (Rządowe Centrum Legislacyjne)
- Akty prawa miejscowego - uwarunkowania prawne, specyfika, rodzaje aktów, procedura stanowienia.

Więcej: www.cpi.com.pl

cpi
centrum promocji informatyki

Bezpieczeństwo procesu publikacji ustaw i rozporządzeń

Przemysław Momot, Michał Tabor

Pomiędzy prawnikami krąży anegdota o rozprawie sądowej, podczas której w wyniku rozbieżności pomiędzy wydrukami z programu LEX i stron sejmowych sąd zadał pytanie do właścicieli serwisów o to, który z zapisów jest prawidłowy. W rzeczywistości każdy prawnik wie, że podstawą i jedynym punktem odniesienia w zakresie prawa powszechnego jest wydany papierowo Dziennik Ustaw. Aktualnie są one drukowane w tysiącach egzemplarzy i rozsyłane do sądów, urzędów oraz trafiają do wielu kancelarii. Z początkiem 2012 roku proces ten ma ulec zasadniczej zmianie, wspomniane dzienniki będą wydawane tylko w kilku egzemplarzach papierowych – do celów archiwalnych, natomiast podstawą i jedynym oficjalnym punktem odniesienia będą ich elektroniczne wersje udostępniane powszechnie w sieci Internet. Jest to moment, aby przyjrzeć się bezpieczeństwu informacji w procesie publikacji aktów normatywnych.

Bezpieczeństwo informacji jest bardzo szerokim zagadnieniem, które wymaga analizy procesów, celów biznesowych i informacji oraz wspierających je aktywów informatycznych pod kątem zagrożeń i niedostatków oraz wynikających z nich ryzyk. W zgodzie z międzynarodowymi standardami i dobrymi praktykami bezpieczeństwo informacji jest rozpatrywane w trzech podstawowych kryteriach skutków utraty: poufności, integralności i dostępności. Fakt, że akty prawne są publicznie dostępne we wszystkich etapach cyklu życia, powoduje, że nie ma sensu rozpatrywanie konsekwencji związanych z uratą poufności i w związku z powyższym zasadnicze znaczenie mają ich **integralność** i **dostępność**.

Zapewnienie integralności ustaw i rozporządzeń ma zasadnicze znaczenie na wszystkich etapach powstawania aktu począwszy od pierwszego projektu, a skończywszy na opublikowanym i udostępnionym dokumencie. W zależności od etapu należy rozpatrywać dodatkowe atrybuty informacji oraz skutki ich utraty. Przykładowo dla opublikowanych już aktów prawnych oprócz integralności gwarantującej niezmienność treści należy również rozpatrywać skutki utraty lub niezapewnienia autentyczności oraz rozliczalności procesu publikacji. Natomiast dla etapów tworzenia aktu istotnym atrybutem będzie rozliczalność podejmowanych działań. Warto w tym miejscu wspomnieć aferę sprzed kilku lat, tzw. „i czasopisma", gdzie zapewnienie integralności, a także niezaprzeczalność dokonywanych przez urzędników modyfikacji projektu aktu stanowiły o bezpieczeństwie prawnym i umożliwiały nielegalne wpływanie na ostateczny kształt stanowionego prawa. Zagadnieniom tym poświęcimy drugą część niniejszego artykułu.

Zapewnienie dostępności aktów nie tylko oznacza działanie serwisów je udostępniających w trybie 24/7/365, ale także zapewnienie tego, że akt zostanie opublikowany na czas, zgodnie z decyzją urzędową. Konieczność zapewnienia ciągłości działania procesów publikujących akty normatywne w wielu przypadkach stanowi o bezpieczeństwie, a nieopublikowanie na czas np. przepisów dotyczących podatku dochodowego do 30 listopada może stanowić ogromne zagrożenie dla budżetu.

Procesy publikacji ustaw i rozporządzeń przebiegają w ten sam sposób i z punktu widzenia tego procesu różnią się jedynie osobą

posiadającą kompetencje do ich ogłoszenia, co oznacza, że będą się różniły podpisem znajdującym się na akcie skierowanym do publikacji. Na potrzeby niniejszego artykułu ograniczę się do opisywania procesu publikacji ustaw. Instytucją odpowiedzialną w imieniu Prezesa Rady Ministrów za przeprowadzenie procesu publikacji jest Rządowe Centrum Legislacji. RCL przyjmuje podpisane przez prezydenta ustawy, redaguje je i nadzoruje ich druk oraz udostępnienie elektroniczne. Niejednokrotnie zdarza się, że wymagane jest opublikowanie ustawy bezzwłocznie, tj. w dniu jej otrzymania lub dnia następnego, zapewnienie ciągłości tego procesu wymaga odpowiedniego przygotowania organizacji i wprowadzeniu odpowiednich zabezpieczeń.

Publikacja aktów w postaci elektronicznej będzie polegała na zastąpieniu druku aktu jego publikacją w elektronicznych serwisach ustawowo do tego przeznaczonych. Stwierdzeniem faktu publikacji będzie zatem nie pojawienie się papierowej wersji dziennika w punktach dystrybucji, ale pojawienie się jego wersji elektronicznej w publicznie dostępnych serwisach elektronicznych. Zapewnienie ciągłości funkcjonowania procesu publikacji wymaga wskazania krytycznych podprocesów związanych z publikacją, którymi są:

- przyjęcie ustawy do publikacji i weryfikacja jej integralności i autentyczności;
- zredagowanie ustawy w ramach dziennika;
- zabezpieczenie integralności i autentyczności dziennika;
- publikacja dziennika w serwisie udostępniającym;
- zabezpieczenie niezaprzeczalności działań związanych z wyżej wymienionymi podprocesami.

Brak możliwości realizacji któregokolwiek z powyższych elementów może spowodować brak publikacji wymaganych przepisów na czas lub publikacja zmanipulowanego przepisu, a co za tym idzie, bardzo poważne konsekwencje prawne. Dlatego też obowiązkiem RCL jest takie zorganizowanie tych procesów i wdrożenie procedur zapewniających ciągłość działania, aby zminimalizować ryzyko poprawnego zakończenia procesu publikacji aktu w określonym terminie.

Wdrożenie rozwiązania mającego na celu zapewnienie ciągłości działania musi uwzględniać wszystkie elementy organizacji, infrastruktury i systemów teleinformatycznych wykorzystywanych w procesie publikacji aktów prawnych. Rządowe Centrum Legislacji, przygotowując się do realizacji obowiązku publikacji elektronicznej, powinno uwzględniać opracowanie takiego planu ciągłości działania, który zapewnia:

- przeniesienie działalności w inne miejsce w przypadkach krytycznych,
- procedury komunikacyjne,
- redundancję infrastruktury i jej odporność na zewnętrzne i wewnętrzne awarie.

Realizując powyższe należy przeprowadzić analizę i ocenę ryzyka, która pokaże na jakie scenariusze ryzyka organizacja powinna być gotowa. Czy przykładowo zamieszki w centrum Warszawy nie spowodują braku możliwości publikacji wymaganych zmian przepisów.

Przykładem błędnego rozumienia wdrożenia mechanizmów ciągłości działania jest ograniczenie się organizacji do ustanowienia ośrodka zapasowego, a czasem wyłącznie do zapewnienia redundancji urządzeń. Najczęściej nie zostaje również przeprowadzona analiza wpływu zdarzeń na osiągnięcie celów biznesowych. Ciągłość działania powinna być objęta analizą ryzyka, a plany zapewnienia ciągłości działania powinny uwzględniać bezpieczeństwo informacji. Plany powinny zawierać odpowiednie procedury uwzględniające warunki ich

uruchomienia, odpowiednią strukturę organizacyjną wraz z przypisanymi obowiązkami na wypadek wdrożenia planów ciągłości działania, a osoby odpowiedzialne za realizację planów powinny być regularnie szkolone. Plany powinny być też regularnie testowane. Tylko takie podejście do zagadnienia ciągłości działania zapewni RCL-owi bezpieczne awaryjne procesy publikacji aktów prawnych.

Kluczowym warunkiem sukcesu w zakresie budowy i ustanowienia systemu zarządzania bezpieczeństwem informacji jest zaangażowanie najwyższego kierownictwa. Wsparcie kierownictwa na każdym etapie opracowania systemu zarządzania bezpieczeństwem informacji połączone z managerskim spojrzeniem na działalność biznesową organizacji oraz managerską kontrolą postępów projektu pozwoli docelowo na zapewnienie, że przekazany do publikacji akt będzie zawsze opublikowany na czas, a zaproponowane rozwiązania są rzeczywiste i możliwe do realizacji Wdrożenie takiego systemu wymaga szczegółowej analizy procesów, posiadanych i wytwarzanych zasobów i dopiero w oparciu o analizę kosztów i ryzyka ustanowienie zasad oraz wdrożenie zabezpieczeń organizacyjnych i technicznych.

Zarządzanie bezpieczeństwem nie może ograniczyć się tylko do ustanowienia mechanizmów ciągłości działania, ponieważ wszystkie elementy związane z bezpieczeństwem wzajemnie się przenikają i są od siebie zależne. Bezpieczeństwo procesu publikacji to także zadbanie o to, żeby każde działanie w procesie publikacji aktu było kontrolowane i umożliwiało po pierwsze wykrycie nieuprawnionej ingerencji, a po drugie wskazywało źródło każdej czynności. Zbudowanie zabezpieczeń organizacyjnych i technicznych zapewniających, że opublikowana ustawa będzie wiarygodna, wymaga szczegółowej analizy procesu publikacji oraz zastosowania dostępnych technologii. Jednocześnie takie rozwiązanie musi uwzględniać łatwość dostępu i weryfikacji wiarygodności opublikowanej ustawy, bez konieczności korzystania ze specjalistycznych narzędzi i specjalistycznej wiedzy.

Zapewnienie wszystkich wspomnianych powyżej atrybutów bezpieczeństwa informacji zawartych w publikowanych aktach prawnych pozwoli obywatelom, urzędom i sądom na posługiwanie się nimi z pełnym zaufaniem, że jest to akt ustanowiony.

Bardzo ważnym składnikiem procesu publikacji jest gromadzenie i właściwe zabezpieczenie dowodów wykonanych działań. Aby dowody te nie mogły zostać podważone, powinny być odpowiednio zabezpieczone przed utratą integralności. Muszą również być dostępne w sposób czytelny dla wszystkich instytucji uprawnionych do weryfikacji poprawności realizacji wspomnianego procesu, jak również dla odpowiednich służb w przypadku wykrycia nadużycia.

Wydawałoby się, że najbardziej wiarygodnym aktem prawnym przeznaczonym do publikacji powinien być dokument podpisany przez kompetentną osobę w państwie, czyli prezydenta dla ustawy lub ministra dla rozporządzenia. Jednak taki prosty mechanizm ma kilka wad. Należy pamiętać, że RCL jest zobowiązany do opublikowania aktu w formalnym formacie dziennika urzędowego wraz z dołączonymi informacjami o dacie publikacji. Z tego powodu zasadnym jest, aby dokument zawierający opublikowaną ustawę nie był tym, który prezydent podpisał, a jedynie dokumentem identycznym co do treści i utworzonym na podstawie podpisanej przez prezydenta ustawy. Dokument taki powinien być jednak odpowiednio zabezpieczony za pomocą mechanizmów kryptograficznych gwarantujących jego integralność i autentyczność.

Już teraz podpis elektroniczny służy do zabezpieczenia publikowanych ustaw. Publikowaną treść ustawy podpisuje bezpiecznym podpisem elektronicznym weryfikowanym kwalifikowanym certyfikatem (podpisem kwalifikowanym) upoważniony dyrektor Rządowego Centrum Legislacji. Jednak podpis kwalifikowany nie jest najlepszym narzędziem dla zapewnienia autentyczności i integralności publikowanych aktów.

Podstawową wadą podpisu kwalifikowanego jest to, że nie niesie za sobą uprawnień osoby posługującej się tym podpisem do publikacji dziennika. A więc osoba posługująca się ustawą nie ma wiedzy, czy podpis złożony pod jej treścią został wykonany zgodnie z jej uprawnieniami, a co za tym idzie, czy posiadany akt jest autentyczny. Dodatkowym elementem jest to, że w żaden sposób technologia nie wspiera kontrolowania tego, czy podpis kwalifikowany został złożony zgodnie z obowiązującą procedurą, czy przypadkiem dokument nie został podpisany poza systemem RCL.

Kolejny problem rodzi specyfika podpisu kwalifikowanego, który dla prawidłowej weryfikacji wymaga, aby certyfikat podpisującego był ważny. Wiadomym problemem jest to, że w momencie wygaśnięcia certyfikatu lub jego unieważnienia (np. gdy podpisujący zmienia miejsce pracy) weryfikacja podpisu jest utrudniona. Oczywiście występują mechanizmy znakowania czasem i uzyskania postaci archiwalnej podpisu, ale po pierwsze nie wszystkie aplikacje weryfikujące podpis poprawnie umieją je zinterpretować, a po drugie podpis oznakowany czasem też wygasa.

Oczywiście należy tutaj uznać, że podstawowym zabezpieczeniem opublikowanych ustaw pod względem integralności jest ich postać źródłowa znajdująca się na serwerach Dziennika Ustaw oraz wielość kopii znajdująca się w urzędach i kancelariach. Jeżeli ktoś ma wątpliwości dotyczące autentyczności i integralności posiadanej ustawy, to na podstawie jej sygnatury weryfikuje jej tekst źródłowy. Tutaj warunkiem jest zapewnienie autentyczności źródła na podstawie mechanizmów, tj. serwerów SSL.

Jednak prawdziwym zabezpieczeniem opublikowanych aktów normatywnych, które powinny móc występować w środowisku niepodłączonym do sieci i oddalonym od systemu dziennika ustaw, jest odpowiednie zastosowanie zaawansowanego podpisu elektronicznego RCL, tzw. pieczęci elektronicznej, której dane do składania zabezpieczone byłyby urządzeniami HSM. Wymagane jest, aby złożenie pieczęci kontrolowane było odpowiednimi procedurami organizacyjnymi i technicznymi. Pieczęć taka mogłaby zachowywać wieloletnią ważność, z niewielkim ryzykiem, że nastąpią przesłanki do jej unieważnienia.

Dodatkowym mechanizmem, który jest powszechnie stosowany na świecie, jest wydawanie automatycznych odpisów z dziennika ustaw, których autentyczność i integralność zapewnia pieczęć elektroniczna. Zaletą tego mechanizmu jest to, że ważność odpisu pozostaje w mocy w okresie ważności certyfikatu, tj. przez okres kilkunastu miesięcy. Niepotrzebne jest znakowanie czasem i w przypadku wygaśnięcia ważności certyfikatu pobiera się kolejny odpis – ważny przez kolejny okres.

Nowoczesne techniki umożliwiają szereg zastosowań mechanizmów podpisu elektronicznego w sposób, który nie tylko zapewni realizację obowiązku prawnego, ale przede wszystkim umożliwi łatwe i bezpieczne korzystanie z opublikowanych

aktów normatywnych. Należy zauważyć, że implementacja mechanizmów bezpieczeństwa wymaga gruntownej analizy potrzeb, ryzyka i możliwości, korzystania z najlepszych praktyk i otwarcia na dostępne technologie. Wdrożenie całkowicie elektronicznych dzienników może znacząco ułatwić i zmniejszyć koszty sądów i urzędów w zakresie dostępu do źródła prawa, ale zastosowanie nieprzemyślanych rozwiązań może szybko zmusić administrację do powrotu do papierowego dziennika.

Przemysław Momot - architekt bezpieczeństwa systemów teleinformatycznych i systemów zarządzania bezpieczeństwem informacji administracji publicznej. Wieloletni audytor systemów teleinformatycznych w zakresie bezpieczeństwa informacji.

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.

Zapraszamy do udziału

SEMINARIUM
„RYZYKO DECYZJI W ADMINISTRACJI RZĄDOWEJ I SAMORZĄDOWEJ I JEGO DOPUSZCZALNE GRANICE”
26 lipca 2011 r., Warszawa

Prowadzenie obrad: dr inż. Agnieszka Gryszczyńska, Katedra Prawa Informatycznego UKSW.

W PROGRAMIE:

- Procedury decyzyjne w administracji publicznej.
  prof. dr hab. Małgorzata Jaśkowska (Naczelny Sąd Administracyjny, kierownik Katedry Postępowania Administracyjnego UKSW)
- Dopuszczalne ryzyko w podejmowaniu decyzji administracyjnych i jego granice.
  Mateusz Błachucki (Instytut Nauk Prawnych PAN)
- Odpowiedzialność karno-prawna, administracyjna i cywilna za nieprzestrzeganie przepisów o ochronie danych osobowych oraz za niedopuszczalne przetwarzanie danych osobowych.
  dr Gerard Karp (Wierzbowski Evershedes)
- Metody potwierdzania tożsamości użytkowników elektronicznych usług publicznych.
  dr inż. Agnieszka Gryszczyńska (Katedra Prawa Informatycznego, UKSW)
- Regulacje prawne określające zakres i specyfikę odpowiedzialności osobistej i majątkowej funkcjonariuszy publicznych - ze szczególnym uwzględnieniem przepisów ustawy z 20/01/2011.

Więcej: www.cpi.com.pl

cpi
centrum promocji informatyki

Powszechny dostęp do orzeczeń sądowych

Kazimierz Chojna

Powszechny dostęp do orzecznictwa sądowego stanowi prawo przysługujące każdemu obywatelowi. Prawo to wiąże się nierozerwalnie z postulatem jawności postępowania sądowego, wyrażonym w art. 45 Konstytucji Rzeczypospolitej Polskiej oraz prawie do uzyskiwania informacji o działalności organów władzy publicznej, wynikającym z art. 61 ust. 1 Konstytucji. Dostęp do informacji wytworzonych przez podmioty, tzw. *imperium*, jest także jednym z podstawowych praw Europejskiej Karty Praw Człowieka, wyrażonym w art. 6 ust. 1 tego aktu. Na gruncie ustawodawstwa krajowego niższej rangi uprawnienie polegające na dostępie do orzeczeń sądów powszechnych i administracyjnych jest zawarte w normach ustaw o dostępie do informacji publicznej[1] oraz w ustawach regulujących kwestie ustrojowe sądownictwa[2]. Bardzo istotne miejsce w kwestii rozważań nad powszechną dostępnością orzeczeń sądowych ma definicja pojęcia informacji publicznej, wyłożonej przez sądownictwo administracyjne, zgodnie z którą informacją publiczną jest „każda wiadomość wytworzona lub odnoszona do władz publicznych"[3].

Szeroka i powszechna dostępność orzeczeń sądowych stanowi *modus vivendi* demokratycznego państwa prawa. Silna i w dużym stopniu niezależna od pozostałych władz pozycja tzw. trzeciej władzy jest ograniczana przede wszystkim przez kontrolę jaką sprawuje opinia publiczna. Sądownictwo, mimo iż jest w swych wyrokach niezależne, a sędziowie niezawiśli, *de facto* ponoszą przed społeczeństwem odpowiedzialność za efekty swej pracy, które następnie weryfikuje władza ustawodawcza poprzez proces stanowienia prawa. Tylko dzięki prawu dostępu do informacji publicznej sądy oraz urzędy nie stają się instytucjami oddzielonymi od obywatela i cynicznie wykorzystującymi władzę, jaka została im powierzona przez społeczeństwo, lecz poprzez poczucie stałej kontroli stają się organami bardziej obiektywnymi i praworządnymi. Nawet jeżeli opisywane cechy nie są bezpośrednio odczuwalne, łatwo można byłoby sobie wyobrazić stan władz państwowych pozbawionych kontroli.

Inne korzyści powiązane z publiczną dostępnością orzeczeń sądowych są związane z doniosłą rolą, jaką odgrywają w polskim systemie prawnym orzeczenia Sądu Najwyższego (SN), Trybunału Konstytucyjnego (TK) oraz Naczelnego Sądu Administracyjnego (NSA). Jedną z ról tych naczelnych organów państwa jest precyzowanie prawa w obszarach, w których ustawodawca pozostawił wątpliwości lub dowolność w jego stosowaniu. Szczególnie istotną dla obywatela i innych podmiotów prawa wydaje się działalność SN i NSA. Wykładnia legislacji tworzona przez te sądy ma bardzo duży wpływ na pojmowanie prawa przez jego adresatów. Często

1 Ustawa o dostępie do informacji publicznej z 6 września 2001 r. Dz. U. Nr 112 poz. 1198 w szczególności art. 1 ust. 1 ustawy.

2 Chodzi tu przede wszystkim o ustawę Prawo ustroju sądów powszechnych z 27 lipca 2001 r. Dz. U. Nr 98 poz. 1070 z pożń. zm. oraz ustawę Prawo ustroju sądów administracyjnych z 2002 r. Dz. U. Nr 153 poz. 1269 z pożn. zm.

3 Wojewódzki Sąd Administracyjny w Warszawie, sygn. VIII SAB/Wa 5/2008

wyroki mają charakter wręcz prawotwórczy i zasadniczo zmieniają sytuację podmiotu praw i obowiązków. Bardzo dobrą ilustracją dla takiego stanu rzeczy jest orzecznictwo NSA, które weryfikuje niedoskonałe przepisy prawa podatkowego oraz ogranicza niejednokrotnie nieadekwatną działalność urzędów skarbowych.

Niewątpliwie rozwój Internetu oraz technologii cyfrowych znacznie ułatwia proces publikacji orzeczeń sądowych. Forma elektroniczna pozwala na duże oszczędności oraz zwiększenie dostępności do wyroków i decyzji. Najlepszym przykładem jest popularyzacja komercyjnych baz danych zawierających akty normatywne oraz orzecznictwo.

Praktyka dostępu do orzeczeń sądowych

Postulat dostępu do informacji publicznej, który władze publiczne powinny odczytywać jako obowiązek, jest różnie realizowany przez poszczególne elementy władzy sądowniczej. Obecny stan bardzo dobrze ukazuje raport pt. *Publiczna Dostępność Orzeczeń Sądowych*[4]. Jednym z podstawowych wniosków płynących z tej pracy jest brak jednolitości w procesie publikacji orzeczeń sądowych. Autorzy raportu zauważają, że najlepiej z tej funkcji wywiązują się TK oraz sądownictwo administracyjne, które od ponad dekady publikują wszystkie bieżące orzeczenia oraz wprowadzają do obiegu orzeczenia dawniejsze, które są istotne dla praktyki prawa. TK i NSA używają w tym celu przede wszystkim własnych stron internetowych oraz w mniejszym zakresie formy papierowej.

Zdecydowanie gorzej ze swego obowiązku wywiązuje się SN, który publikuje jedynie nieznaczną część swego orzecznictwa. Jako podstawowe narzędzie, którego używa SN do udostępniania swoich wyroków, autorzy raportu wymieniają *Zeszyty SN*[5], które są zbiorami urzędowymi. Wyboru zamieszczonych orzeczeń dokonują sami sędziowie. Najważniejszym kryterium, według którego dokonywana jest publikacja, to precedensowość oraz istotne znaczenie orzeczenia. Strona internetowa SN zawiera jedynie część orzecznictwa – mniejszą niż ta umieszczona w *Zeszytach*. Na uwagę zasługuje Baza Danych SN o nazwie Supremus, która stale jest zasilana obecnymi oraz dawniejszymi orzeczeniami, ale nie zawiera orzeczeń wszystkich Izb SN.

Sądy Apelacyjne publikują jedynie część orzeczeń, wybranych ze względu na znaczenie dla praktyki i doktryny. Wyroki zamieszczone w Internecie pokrywają się w wyborze z tymi, które zostały opublikowane w formie papierowej.

Sądy Okręgowe wydały w 2009 r. ok. 800 tys. orzeczeń i co do zasady ich nie publikują.[6] Sądy Rejonowe, z dorobkiem ok. 11 mln rocznie, również nie publikują wyroków, uzasadniając to małym zainteresowaniem ich orzecznictwem (innego zdania są adwokaci).

Powyższe dane i konferencja podsumowująca Raport[7] ukazują, że sądy powszechne najgorzej realizują zasadę jawności postępowania sądowego. Szczególnie dużym problemem jest brak dostępu do orzeczeń SN i Sądów Apelacyjnych, na które istnieje duże zapotrzebowanie. Najmocniej krytykowane są braki po stronie SN, który z racji swojego podstawowego zadania, czyli sprawowania nadzoru nad działalnością sądów powszechnych w zakresie orzekania, *de facto* przybiera

4 Raport został przygotowany w 2010 r. przez Forum Obywatelskiego Rozwoju, Helsińską Fundację Praw Człowieka i Kolegium Prawa Akademii im. Leona Koźmińskiego.
5 Zeszyty są publikowane w ramach Izb SN np. „Orzecznictwo SN Izba Cywilna".
6 Wyjątek stanowią SO w Białymstoku oraz Gliwicach.
7 Relacja z konferencji w ALK – portal naszawokanda.pl.

rolę prawotwórczą. W praktyce SN ma wielki udział w praktyce wykładni i stosowania przepisów prawa przez sądy powszechne.

Niewidzialna ręka rynku

Podobnie jak w każdym innym sektorze gospodarki, tak i w sektorze usług prawniczych istnieje zasada, że rynek nie lubi próżni. W odpowiedzi na braki jednolitej publicznej bazy danych, która zawierałaby orzecznictwo różnych sądów i trybunałów, powstają liczne komercyjne bazy. Zdecydowana większość z nich wymaga uiszczenia opłaty okresowej w zamian za dostęp do informacji. Zawarte w nich orzecznictwo w głównej mierze pokrywa się z publikacjami sądów zamieszczonymi w formie papierowej lub zawartymi na stronach internetowych. Jednakże i w tych bazach zawarta jest tylko część orzeczeń – mało który przedsiębiorca wnosi do prezesa sądu o udostępnienie orzeczenia, które mógłby następnie zamieścić w bazie danych. Naturalnie, opisywane bazy nie wypełniają zasady dostępności informacji publicznych, ich odpłatność, często związana z wysoką ceną, powoduje, że wielu obywateli, wśród nich studentów prawa czy administracji, nie ma możliwości poznania interesującego ich orzeczenia. Odpowiedzią na taki stan rzeczy są liczne fora internetowe, na których omawiane oraz zamieszczane są orzeczenia oraz akty normatywne. Informacje tam zawarte często są niepełne, a nawet błędne.

Casus naszawokanda.pl

Rozwój technologii cyfrowych i stale poszerzający się dostęp do Internetu powodują, że praktyka i doktryna prawa jest coraz liczniej i lepiej jakościowo reprezentowana na stronach internetowych. Bezpłatny dostęp do źródeł prawa, w szczególności rangi ustawowej, stał się normą. Na dużą uwagę zasługuje w tej materii działalność Kancelarii Sejmu, która na stronie internetowej parlamentu[8] opublikowała znaczną część ustaw i wiele rozporządzeń. Nawet jeżeli osoba szukająca konkretnego aktu prawnego nie znajdzie go na stronach w domenie gov.pl, istnieje duża szansa, że odnajdzie taki akt za pomocą popularnych wyszukiwarek jak np. Google. W dużo gorszej sytuacji znajdzie się osoba, która próbuje odnaleźć orzeczenie sądu – sporo wysiłku może kosztować ustalenie, że pełnego tekstu nie ma w sieci, a omówienie jest niedokładne.

W tej kwestii warto zwrócić uwagę na portal naszawokanda.pl. Pod tym adresem można odnaleźć nie tylko akty normatywne w formie ustaw i rozporządzeń, ale również orzecznictwo sądów i trybunałów oraz Urzędu Zamówień Publicznych. Jest to chlubny wyjątek od zasady „niedostępności orzeczeń". To proste narzędzie będzie pomocne wszystkim prawnikom oraz osobom, które jedynie doraźnie szukają informacji prawnych. Powyższy portal stanowi przykład zjawiska przejmowania funkcji właściwych sektorowi publicznemu przez sektor prywatny. Bezpłatny dostęp do orzeczeń sądowych jest pomocny dla studentów studiów prawniczych i z nimi powiązanych. Student prawa powinien już od pierwszego roku nauki uczyć się posługiwania orzecznictwem. Każde przeczytane uzasadnienie do wyroku pozwala lepiej zrozumieć system sądownictwa oraz specyficzny meta-język prawniczy, którym posługuje się władza sądownicza, różny nie tylko od języka codziennego, ale też od klasycznego języka prawnego i prawniczego. Naszawokanda.pl wspomaga również rozwój doktryny nauk prawnych na wyższym poziomie. Czy można sobie wyobrazić glosę bez orzeczenia? Albo dyskurs na gruncie prawa konstytucyjnego bez znajomości wyroków TK?

Ważny jest również udział takich projektów w rozwoju małych i mikroprzedsiębiorstw. Często te formy działalności gospodarczej nie mogą pozwolić sobie na zatrudnienie tzw. in-house-lawyer czy nawet na stałą obsługę prawną. Korzystanie z usług prawniczych przez takie podmioty odbywa się najczęściej

8 www.sejm.gov.pl

ad hoc w związku ze zbyciem czy nabyciem znacznego majątku albo w razie problemów prawnych i konieczności występowania przed sądami. Informacji na temat prawa zamówień publicznych czy prawa ochrony konsumenta i konkurencji osoby zarządzające przedsiębiorstwami muszą szukać na własną rękę. Tym samym zmniejsza się pewność obrotu prawnego, a przedsiębiorca naraża się na większe ryzyko, a czasami na poważne straty materialne. W takich przypadkach bardzo istotne jest istnienie źródła szerokiej i pewnej informacji prawnej dostępnej w Internecie. Wspomniany portal internetowy posiada w swojej bazie orzecznictwo takich organów naczelnych i centralnych jak: NSA, WSA, SOKiK czy decyzje Prezesa Urzędu Zamówień Publicznych i Prezesa Urzędu Ochrony Konkurencji i Konsumentów. Te zasoby są w stanie zaspokoić wiedzę przedsiębiorców i wzmocnić respektowanie przez nich przepisów prawa.

Naszawokanda.pl zawiera ponad pół miliona orzeczeń, a ta liczba stale rośnie. Kluczowym elementem portalu jest sprawna wyszukiwarka orzeczeń sądowych, która pozwala w szybkim czasie odnaleźć konkretne orzeczenie, nie znając jego sygnatury. Szczególnie istotne są możliwości przeszukiwania zasobów pochodzących z SN, bowiem oficjalna baza danych Supremus nie ma funkcji szukania według słów kluczowych czy rodzajów orzeczenia. Portale takie jak naszawokanda.pl to dobry przykład inicjatywy prywatnej, która wyposażona w znacznie mniejsze środki finansowe jest w stanie przejąć funkcję właściwą dla organów publicznych i ponadto wykonać ją w lepszy jakościowo sposób. Można się tym samym spodziewać, że urzędnik np. władz samorządowych szukający orzeczenia istotnego ze względów zawodowych wybierze bazę danych nie państwową, lecz prywatną, ze względu na jej większy zasób i profesjonalizm.

Synteza

Powszechny dostęp do treści orzeczeń sądowych oraz administracyjnych stanowi jeden z filarów demokratycznego państwa prawa. Pomimo stosunkowo dobrego ustawodawstwa normującego tę kwestię nie wszystkie podmioty sektora publicznego poprawnie wywiązują się ze swojego obowiązku polegającego na jak najszerszym dostępie do informacji publicznej. Nawet instytucje wyposażone w duże środki finansowe, jak np. SN, nie dokonały pełnej publikacji swojego orzecznictwa[9]. Sytuacja ta budzi pewne zaniepokojenie, gdy administracja państwowa dysponuje Internetem oraz nowoczesnymi technologiami cyfrowymi. Tymczasem organy nie są w stanie spełnić obowiązku ustawowego.

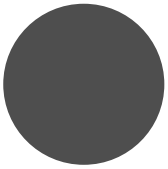
W związku z biernością niektórych instytucji publicznych oraz brakiem całościowego, systemowego rozwiązania, które pozwalałoby na dostęp do aktów normatywnych oraz orzeczeń sądowych, sektor prywatny przejmuje rolę właściwą dla państwa. Często jednak dostęp do komercyjnych baz danych wiąże się z wysoką opłatą, której nie może ponieść przeciętny obywatel, a w szczególności osoba edukująca się w zakresie prawa czy administracji.

Na rynku informatyczno-prawnym zaczynają się pojawiać podmioty prywatne, które skutecznie realizują zasadę powszechnego dostępu do informacji publicznej, czyniąc to w pewnym zakresie bezpłatnie, zwiększając tym samym pewność obrotu prawnego oraz wiedzę społeczeństwa na temat prawa. Pozytywnym przykładem jest portal internetowy naszawokanda.pl.

Kazimierz Chojna jest współpracownikiem portalu naszawokanda.pl.

9 W sposób, który pozwalałby osobom zainteresowanym na szybki i prosty dostęp – samo ogłoszenie nie jest procesem wystarczającym.

Nowe zasady prowadzenia ewidencji ludności



Katarzyna Czajkowska-Matosiuk

Dnia 1 stycznia 2011 r. weszło w życie rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 27 grudnia 2010 r. w sprawie trybu przekazywania danych pomiędzy organami prowadzącymi ewidencję ludności oraz powiadamiania o nadaniu numeru PESEL (Dz. U. Nr 257, poz. 1742). Przewiduje ono, iż przekazywanie danych pomiędzy organami gmin, wojewodami oraz ministrem właściwym do spraw wewnętrznych będzie się odbywało przy wykorzystaniu środków komunikacji elektronicznej.

Luka w prawie

Na podstawie nowelizacji ustawy o ewidencji ludności i dowodach osobistych z dnia 11 kwietnia 2001 r. (Dz. U. Nr 43, poz. 476) przeprowadzono **likwidację systemów kartotecznych**, w tym kart osobowych mieszkańców. Zmiana ta spowodowała, iż zabrakło podstawy prawnej do przekazywania danych pomiędzy organami prowadzącymi ewidencję ludności oraz powiadamiania o nadaniu numeru PESEL przy wykorzystaniu systemów teleinformatycznych.

W związku z tym konieczne stało się wprowadzenie regulacji, która zagwarantowałaby organom prowadzącym ewidencję niezwłoczne pozyskiwanie zaktualizowanych danych oraz zgodność danych zawartych w gminnych i wojewódzkich zbiorach meldunkowych i zbiorze PESEL.

Zakres nowej regulacji

Realizacji powyższych celów służyć ma właśnie nowe rozporządzenie, które w sposób szczegółowy określa:

1) tryb przekazywania pomiędzy ministrem właściwym do spraw wewnętrznych, wojewodą oraz organami gmin danych ze zbiorów meldunkowych oraz zbioru PESEL,
2) tryb powiadamiania o nadaniu numeru PESEL.

W rozporządzeniu tym zrezygnowano ze wszystkich zapisów dotychczas obowiązującego rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 20 grudnia 2002 r. w sprawie trybu przekazywania danych pomiędzy organami prowadzącymi ewidencję ludności oraz powiadamiania o nadaniu numeru PESEL (Dz. U. Nr 236, poz. 1996).

Poprzednie przepisy regulowały problematykę przekazywania danych odnoszących się do kartotecznych systemów ewidencji ludności lub do elektronicznej formy prowadzania ewidencji ludności wyłącznie jako do możliwości alternatywnej. Natomiast obecnie możliwe jest przekazywanie powiadomienia o nadaniu numeru PESEL wnioskodawcy będącemu płatnikiem składek ubezpieczeniowych lub osobą obowiązaną do posiadania numeru PESEL na podstawie odrębnych przepisów, w formie dokumentu elektronicznego. W nowej regulacji określono również terminy przekazywania informacji pomiędzy poszczególnymi organami tak, aby zapewnić niezwłoczne aktualizowanie gromadzonych danych.

Tryb przekazywania danych pomiędzy ministrem, wojewodą oraz organami gmin

W myśl omawianego rozporządzenia organ gminy wprowadza do gminnego zbioru meldunkowego dane ze zbiorów danych:

- stałych mieszkańców,
- byłych mieszkańców,
- obywateli polskich i cudzoziemców zameldowanych na pobyt czasowy trwający ponad 3 miesiące.

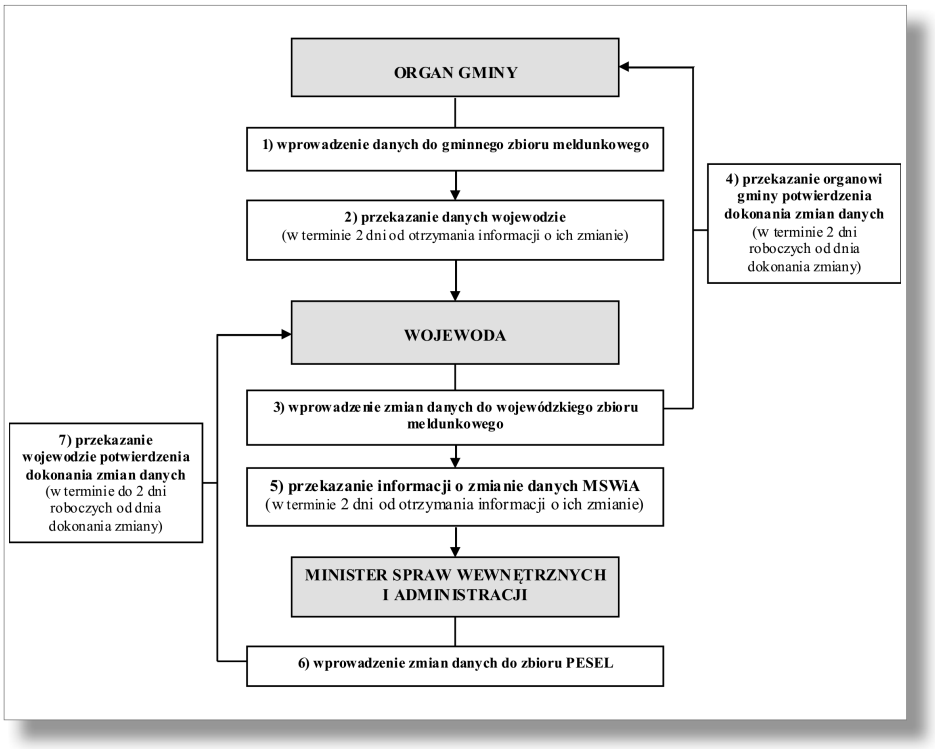
Następnie w terminie do 2 dni roboczych od dnia otrzymania informacji o zmianie tych danych organ gminy przekazuje je wojewodzie.

Wojewoda wprowadza zmiany tych danych w wojewódzkim zbiorze meldunkowym i przekazuje organowi gminy potwierdzenie ich dokonania. Przekazanie potwierdzenia przez wojewodę powinno nastąpić niezwłocznie, jednak nie później niż w terminie do 2 dni roboczych od dnia dokonania takiej zmiany.

Po dokonaniu tej czynności wojewoda w terminie do 2 dni roboczych od dnia otrzymania informacji o zmianie tych danych przekazuje Ministrowi Spraw Wewnętrznych i Administracji informację o wprowadzonych zmianach w celu aktualizacji zbioru PESEL.

Z kolei Minister wprowadza zmiany w zbiorze PESEL i przekazuje niezwłocznie (nie później niż do 2 dni roboczych od dnia dokonania takiej zmiany) właściwemu wojewodzie potwierdzenie dokonania tych zmian.

Przekazywanie danych pomiędzy ministrem, wojewodą oraz organami gmin odbywa się w sposób uniemożliwiający dostęp do nich osób nieupoważnionych.



Schemat 1. Tryb przekazywania danych pomiędzy ministrem, wojewodą oraz organami gmin

Tryb przekazywania danych pomiędzy ministrem, wojewodą oraz organami gmin ilustruje Schemat 1.

Tryb zameldowania osoby na pobyt stały

Organ gminy, który dokonuje zameldowania osoby na pobyt stały, zawiadamia o nowym miejscu pobytu organ gminy właściwy ze względu na poprzednie miejsce pobytu stałego tej osoby.

Zawiadomienie takie powinno zawierać następujące dane meldowanej osoby:
1) imię (imiona) i nazwisko,
2) nazwisko rodowe,
3) imiona i nazwiska rodowe rodziców,
4) datę i miejsce urodzenia,
5) numer PESEL,
6) adres nowego miejsca zameldowania na pobyt stały,
7) datę zameldowania,
8) nazwę, serię i numer dokumentu stwierdzającego tożsamość,
9) oznaczenie organu, który go wydał.

Organ gminy właściwy ze względu na poprzednie miejsce pobytu stałego, po otrzymaniu zawiadomienia, przekazuje organowi nowego miejsca pobytu stałego następujące dane tej osoby:
1) nazwisko i imiona,
2) nazwisko rodowe,
3) nazwiska i imiona poprzednie,
4) imiona i nazwiska rodowe rodziców,
5) datę i miejsce urodzenia,
6) stan cywilny,
7) numer aktu urodzenia i oznaczenie urzędu stanu cywilnego, który ten akt sporządził,
8) płeć,
9) numer PESEL,
10) obywatelstwo (data nabycia obywatelstwa polskiego, data utraty obywatelstwa polskiego),
11) poprzednie adresy zameldowania na pobyt stały wraz z określeniem okresu zameldowania,
12) adres zameldowania na pobyt czasowy trwający ponad 3 miesiące wraz z określeniem okresu zameldowania,
13) tryb wymeldowania,
14) serię i numer aktualnego dowodu osobistego oraz serie i numery poprzednich dowodów osobistych, daty ich wydania i daty ważności oraz oznaczenie organów wydających.

W przypadku osób, które zawarły małżeństwo, organ poprzedniego miejsca pobytu stałego przekazuje także:
1) imię i nazwisko rodowe małżonka oraz jego numer PESEL,
2) datę zawarcia związku małżeńskiego,
3) numer aktu małżeństwa i oznaczenie urzędu stanu cywilnego, który ten akt sporządził,
4) datę rozwiązania związku małżeńskiego,
5) sygnaturę akt i oznaczenie sądu, który rozwiązał małżeństwo,
6) datę zgonu małżonka,
7) numer aktu zgonu i oznaczenie urzędu stanu cywilnego, który ten akt sporządził.

Tryb zameldowania osoby na pobyt czasowy

Organ gminy dokonujący zameldowania osoby na pobyt czasowy trwający ponad 3 miesiące przekazuje organowi gminy właściwemu ze względu na miejsce jej pobytu stałego następujące dane tej osoby:
1) nazwisko i imiona,
2) nazwisko rodowe,
3) nazwiska i imiona poprzednie,
4) imiona rodziców,
5) nazwiska rodowe rodziców,
6) datę i miejsce urodzenia,
7) numer PESEL,
8) rodzaj, serię i numer dokumentu tożsamości,
9) adres miejsca pobytu czasowego i czas jego trwania.

W przypadku, gdy aktualnie osoba taka nie posiada miejsca pobytu stałego organ meldujący na pobyt czasowy przekazuje powyższe dane organowi gminy właściwemu ze względu na ostatnie miejsce pobytu stałego.

Z kolei organ gminy dokonujący wymeldowania osoby z miejsca pobytu czasowego trwającego ponad 3 miesiące przed upływem okresu zgłoszonego przy zameldowaniu przekazuje organowi gminy właściwemu ze względu na miejsce jej pobytu stałego następujące dane tej osoby:

1) nazwisko i imiona,
2) nazwisko rodowe,
3) nazwiska i imiona poprzednie,
4) imiona rodziców,
5) nazwiska rodowe rodziców,
6) datę i miejsce urodzenia,
7) obywatelstwo,
8) numer PESEL,
9) rodzaj, serię i numer dokumentu tożsamości,
10) informację o dacie wymeldowania z miejsca pobytu czasowego trwającego ponad 3 miesiące.

W przypadku braku stałego miejsca pobytu takiej osoby powyższe dane należy przekazać organowi gminy właściwemu ze względu na ostatnie miejsce jej pobytu stałego.

Wykorzystanie wydruku z systemu teleinformatycznego

Przekazywanie danych pomiędzy organami gmin powinno odbywać się **z wykorzystaniem wydruku z systemu teleinformatycznego** opatrzonego pieczęcią organu, podpisem i pieczęcią upoważnionego pracownika tego organu.

Organ dokonujący przekazania ma obowiązek uczynić to w terminie do 4 dni roboczych od dnia otrzymania informacji w tym przedmiocie.

Wykorzystanie środków komunikacji elektronicznej

Ponadto procedura przekazywania danych może odbywać się **z wykorzystaniem środków komunikacji elektronicznej** na zasadach określonych w ustawie z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. Nr 64, poz. 565, ze zm.).

Przy zastosowaniu takiego trybu przekazywania danych organ gminy obowiązuje termin do 2 dni roboczych od dnia otrzymania informacji w tym przedmiocie.

Tryb nadawania numeru PESEL

W celu nadania numeru PESEL obywatelom polskim, zameldowanym na pobyt stały lub czasowy trwający ponad 3 miesiące, osobom ubiegającym się o wydanie dowodu osobistego oraz cudzoziemcom zameldowanym na pobyt stały lub czasowy trwający ponad 3 miesiące organ gminy ma obowiązek przekazać Ministrowi Spraw wewnętrznych i Administracji niezbędne dane tych osób. Są to:

1) nazwisko i imiona,
2) nazwisko rodowe,
3) imiona rodziców,
4) nazwisko rodowe matki,
5) płeć,
6) data i miejsce urodzenia,
7) obywatelstwo,
8) adres i miejsce pobytu stałego lub czasowego,
9) rodzaj, seria i numer dokumentu tożsamości.

Przekazanie powinno nastąpić **na informatycznym nośniku danych lub w drodze teletransmisji** w formie dokumentu elektronicznego z aktualnego programu informatycznego.

W przypadku gdy przekazywanie danych w taki sposób jest niemożliwe, organ gminy przekazuje Ministrowi wniosek o nadanie numeru PESEL.

Minister nadaje numer PESEL, a następnie niezwłocznie przekazuje powiadomienie o nadaniu tego numeru organowi gminy, w celu uzupełnienia gminnego zbioru meldunkowego oraz polskiemu konsulowi.

Powiadomienie to przekazywane jest **w formie dokumentu elektronicznego** z wykorzystaniem środków komunikacji elektronicznej na zasadach określonych w ustawie o informatyzacji działalności podmiotów realizujących zadania publiczne.

Jeżeli przekazanie powiadomienia o nadaniu numeru PESEL w formie dokumentu elektronicznego jest niemożliwe, minister powiadamia organ gminy lub polskiego konsula o nadaniu numeru PESEL w formie pisemnej w terminie do 4 dni roboczych od dnia nadania tego numeru.

W powiadomieniu o nadaniu numeru PESEL Minister zamieszcza:
1) imię (imiona) i nazwisko,
2) nazwisko rodowe,
3) imiona rodziców i nazwisko rodowe matki,
4) datę i miejsce urodzenia,
5) rodzaj oraz serię i numer dokumentu stwierdzającego tożsamość,
6) obywatelstwo,
7) numer PESEL,
8) adres zameldowania na pobyt stały albo czasowy trwający ponad 3 miesiące, jeżeli osoba jest zameldowana na terytorium Rzeczypospolitej Polskiej.

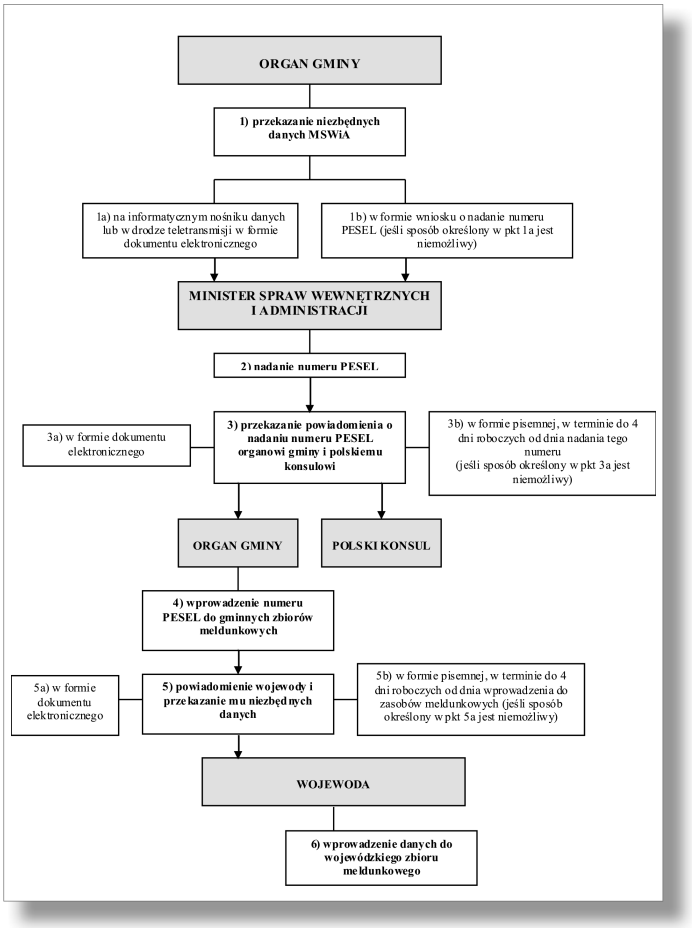
Organ gminy wprowadza numer PESEL do gminnych zbiorów meldunkowych. Następnie powiadamia właściwego wojewodę o nadanym numerze PESEL i przekazuje mu dane niezbędne w celu uzupełnienia wojewódzkiego zbioru meldunkowego, tj.:
1) nazwisko i imiona
2) nazwisko rodowe,
3) nazwiska i imiona poprzednie,
4) imiona rodziców,
5) nazwiska rodowe rodziców,
6) stan cywilny,
7) imię i nazwisko małżonka oraz jego nazwisko rodowe,
8) płeć,
9) datę i miejsce urodzenia,
10) obywatelstwo,
11) numer PESEL,
12) dane dotyczące obowiązku wojskowego, w tym stopień wojskowy, nazwę, serię i numer wojskowego dokumentu osobistego z oznaczeniem wojskowej komendy uzupełnień,
13) adres poprzedniego miejsca pobytu stałego,
14) adres nowego miejsca pobytu stałego,
15) rodzaj, serię i numer dokumentu tożsamości.

Powiadomienie przekazywane jest wojewodzie **w formie dokumentu elektronicznego** z wykorzystaniem środków komunikacji elektronicznej na zasadach określonych w ustawie o informatyzacji działalności podmiotów realizujących zadania publiczne.

W przypadku gdy niemożliwe jest przekazanie wojewodzie powiadomienia w formie dokumentu elektronicznego, organ gminy powiadamia wojewodę o nadanym numerze PESEL w formie pisemnej w terminie do 4 dni roboczych od dnia wprowadzenia numeru do gminnych zasobów meldunkowych.

Procedurę nadawania numeru PESEL ilustruje Schemat 2.

Rozporządzenie wprowadza także możliwość przekazywania powiadomienia o nadaniu numeru PESEL wnioskodawcy będącemu



Schemat 2. Tryb nadawania numeru PESEL

płatnikiem składek ubezpieczeniowych lub osobą obowiązaną do posiadania numeru PESEL na podstawie odrębnych przepisów, w formie dokumentu elektronicznego.

W takim przypadku minister powiadamia wnioskodawcę o nadanym numerze PESEL niezwłocznie po jego nadaniu. Powiadomienie takie jest przekazywane w zależności od żądania wnioskodawcy w formie pisemnej lub w formie dokumentu elektronicznego z wykorzystaniem środków komunikacji elektronicznej na zasadach określonych w ustawie z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne.

Podstawa prawna:

- Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 27 grudnia 2010 r. w sprawie trybu przekazywania danych pomiędzy organami prowadzącymi ewidencję ludności oraz powiadamiania o nadaniu numeru PESEL (Dz. U. Nr 257, poz. 1742),
- Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 20 grudnia 2002 r. w sprawie trybu przekazywania danych pomiędzy organami prowadzącymi ewidencję ludności oraz powiadamiania o nadaniu numeru PESEL (Dz. U. Nr 236, poz. 1996),
- Ustawa z dnia 10 kwietnia 1974 r. o ewidencji ludności i dowodach osobistych (Dz. U. z 2006 r. Nr 139, poz. 993),

- Ustawa z dnia 11 kwietnia 2001 r. o zmianie ustawy o ewidencji ludności i dowodach osobistych oraz o zmianie innych ustaw (Dz. U. Nr 43, poz. 476 ze zm.),
- Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. Nr 64, poz. 565, ze zm.).

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

Zapraszamy do udziału

PODEJŚCIE PROCESOWE W INSTYTUCJACH ADMINISTRACJI PUBLICZNEJ

18-20 lipca 2011 r., Warszawa

Dzisiaj nowoczesny urząd to urząd, który świadczy klientom wysokiej jakości obsługę, szybko i skutecznie reaguje na potrzeby klientów, na bieżąco monitoruje oraz zarządza i usprawnia realizowane procesy, dążąc jednocześnie do optymalizacji kosztów i minimalizowania wydatków publicznych.

Odbiorcy szkolenia:

- samorządy terytorialne (urzędy gmin i miast) - wójtowie, burmistrzowie i prezydenci miast,
- starostwa powiatowe - starości, kadra kierownicza,
- urzędy wojewódzkie - kadra kierownicza UW,
- administracja rządowa - ministerstwa - kadra kierownicza, dyrektorzy departamentów,
- urzędy skarbowe, izby skarbowe - naczelnicy US i dyrektorzy IS,
- ZUS - kadra kierownicza dyrektorzy departamentów,
- Regionalne Dyrekcje Ochrony Środowiska - dyrektorzy, kadra kierownicza,
- Powiatowe i Wojewódzkie Urzędy Pracy - dyrektorzy urzędów.

Cel szkolenia:

- pokazanie od strony praktycznej jak zarządzać procesami w celu podniesienia efektywności i jakości świadczonych usług,
- nauka wdrażania zarządzania procesami tak, aby wytworzyć wewnątrz organizacji presję i nastawienie na usprawnianie procesów,
- metody optymalizacji i usprawniania pracy w urzędzie oraz efektywnie zarządzać kosztami.

Forma szkolenia:

- zajęcia prowadzone są w formie wykładu połączonego z warsztatem,
- prezentacje, dyskusje i ćwiczenia.

Szkolenie jest zaprojektowane w taki sposób, aby prezentować zagadnienia od strony praktycznej, ograniczając do minimum zagadnienia teoretyczne, stanowiące podstawę statystyczną stosowanych metod.

Korzyści, jakie będą mieli Państwo z uczestnictwa w takich warsztatach:

Uczestnicy szkolenia poznają nowoczesne metody i narzędzia zarządzania jakością w urzędzie. Na szkoleniu uczestnicy zdobędą wiedzę z zakresu:

- co to jest proces w urzędzie oraz co to jest jakość pracy w urzędzie,
- efektywnego zarządzania pracą w urzędzie,
- jak zarządzanie jakością wpływa na wzrost satysfakcji klientów urzędów,
- możliwości mierzenia i bieżącego monitorowania jakości pracy urzędników,
- jak można wykorzystywać zarządzanie procesowe do optymalizacji zatrudnienia w urzędzie,
- jakie wskaźniki KPI (*Key Performance Indicators)* można stosować w urzędzie,
- możliwości obiektywnego kontrolowania pracy urzędnika i mierzenia efektów jego pracy,
- mechanizmów eliminujących popełnianie błędów przez urzędników,
- co to jest wydolność procesu, zmienność procesu,
- co zrobić, aby procesy w urzędzie były jednorodne i powtarzalne,
- jak można skracać czas obsługi klienta.

Koszty:

Cena szkolenia: 2 300zł+VAT.
Więcej informacji na temat szkolenia:
http://www.multitrain.pl/home/kalendarium/podejscie-procesowe-w-organizacjach-administracji-publicznej.htm

Kontakt z organizatorem:
Dorota Iwanicka
tel. 22 392 93 91
dorota.iwanicka@multitrain.pl

Zmiany w postępowaniu administracyjnym w 2011 roku

Anita Jackiewicz

Kodeks postępowania administracyjnego został znowelizowany już pięciokrotnie w 2011 r. Zmiany do postępowania administracyjnego wprowadziły odpowiednio ustawy: ustawa z dnia 3 grudnia 2010 r. o wdrożeniu niektórych przepisów Unii Europejskiej w zakresie równego traktowania (Dz. U. Nr 254, poz. 1700); ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. Nr 182, poz.1228); ustawa z dnia 3 grudnia 2010 r. o zmianie ustawy - Kodeks postępowania administracyjnego oraz ustawy - Prawo o postępowaniu przed sądami administracyjnymi (Dz. U. z 2011 r. Nr 6, poz.18); ustawa z dnia 20 stycznia 2011 r. o odpowiedzialności majątkowej funkcjonariuszy publicznych za rażące naruszenie prawa (Dz. U. Nr 34, poz.173); ustawa z dnia 6 sierpnia 2010 r. o dowodach osobistych (Dz. U. Nr 167, poz. 1131) oraz ustawa z dnia 25 marca 2011 r. o ograniczaniu barier administracyjnych dla obywateli i przedsiębiorców (Dz. U. Nr 106, poz. 622).

Zmiana wprowadzona ustawą z dnia 3 grudnia 2010 r. o wdrożeniu niektórych przepisów Unii Europejskiej w zakresie równego traktowania weszła w życie 1 stycznia 2011 r. i związana była z koniecznością zapewnienia realizacji zasady równego traktowania. W art. 24 ustawy określono zmiany w Kodeksie postępowania administracyjnego, polegające na dodaniu art. 145b, który daje możliwość żądania wznowienia postępowania również w przypadku, gdy zostało wydane orzeczenie sądu stwierdzające naruszenie zasady równego traktowania, jeżeli naruszenie tej zasady miało wpływ na rozstrzygnięcie sprawy zakończonej decyzją ostateczną. W takim przypadku podanie o wznowienie można wnieść w terminie jednego miesiąca od dnia uprawomocnienia się orzeczenia sądu. Konsekwencją dodania art. 145b są zmiany wprowadzone odpowiednio w art. 146, art. 147 oraz art. 151. W art. 146 oraz 151 zmianie uległa treść §1 natomiast art. 147 otrzymał nowe brzmienie.

Kolejna zmiana została wprowadzona już następnego dnia, a mianowicie 2 stycznia 2011 r. przez ustawę o ochronie informacji niejawnych. Zmiany zostały wprowadzone odpowiednio w art. 74 §1 oraz art. 82 pkt 2. Wymienione przepisy otrzymały nowe brzmienie w związku z wprowadzeniem podziału informacji niejawnych o klauzuli tajności „tajne" oraz „ściśle tajne" zamiast dotychczasowej ochrony związanej z tajemnicą państwową. Podobny zakres miała zmiana w pkt 2 art.82.

Na dzień dzisiejszy największą i najistotniejszą nowelizacją jest zmiana wprowadzona przez ustawę o zmianie ustawy - Kodeks postępowania administracyjnego oraz ustawy - Prawo o postępowaniu przed sądami administracyjnymi. Obowiązuje ona od 11 kwietnia 2011 r. Celem ustawy zmieniającej było usprawnienie postępowania administracyjnego poprzez wyeliminowanie istniejących luk prawnych, które pozwolą na usprawnienie postępowania administracyjnego poprzez skrócenie procedowania, a także zmotywowanie stron postępowania do czynnego udziału.

Nowe brzmienie art. 7 ma na celu zaktywizowanie stron postępowania. Strona zyskuje uprawnienie do aktywnego wpływania na wyjaśnienie stanu faktycznego sprawy, jednakże nie powinna przerzucać całego ciężaru postępowania na organ prowadzący to postępowanie.

Nową treść otrzymał również art. 8 Kodeksu. Reguluje on zasadę, że postępowanie administracyjne powinno być prowadzone w taki sposób, ażeby budziło zaufanie jego uczestników do władzy publicznej.

Celem wprowadzenia nowego brzmienia dla §1 art. 16 było rozstrzygnięcie istniejących wątpliwości w zakresie decyzji wydawanych przez ministrów i samorządowe kolegia odwoławcze. Doprecyzowano katalog pism ostatecznych.

Nowelizacja art. 24 §1 pkt 5 związana jest z wyłączeniem pracowników, którzy brali udział w wydaniu zaskarżonej decyzji, zarówno pracowników organu I instancji, jak również pracowników urzędów centralnych.

W art. 27 §3 jednoznacznie określono formę prawną wyznaczenia przez ministra właściwego do spraw administracji publicznej innego samorządowego kolegium odwoławczego, a mianowicie dokonuje tego w drodze postanowienia.

Poprzez wprowadzenie nowego brzmienia dla art. 35 i 36 Kodeksu rozciągnięto zakres ich stosowania także na ustawy szczególne, określające krótsze lub dłuższe terminy załatwienia sprawy niż określone w art. 35. Jednocześnie nałożono na organ obowiązek informowania stron o każdym niezałatwieniu sprawy w krótszym terminie i przyczynach tej zwłoki.

Art. 37 przyznaje stronom postępowania administracyjnego prawo skarżenia nie tylko bezczynności organów administracji publicznej, ale również przewlekłości prowadzonego przez te organy postępowania.

Nowelizacja art. 40 wprowadza do Kodeksu regulację w zakresie doręczeń dla strony zamieszkałej lub mającej siedzibę za granicą.

W art. 55 wprowadzono wezwanie telefoniczne albo przy użyciu innych środków łączności.

Dodano nowy art. 61a, który reguluje kwestię rozróżnienia postępowania wstępnego polegającego na wszczęciu lub odmowie wszczęcia postępowania administracyjnego od postępowania właściwego, które kończy się rozstrzygnięciem sprawy co do istoty. Ażeby ujednolicić przepisy Kodeksu w tym zakresie uchylono §3 w art. 157.

Nowe brzmienie przewidziane dla §1 art. 65 oraz §1 i 2 art. 66 miało na celu uregulowanie trybu przekazywania podania do organu właściwego w sprawie przez organ niewłaściwy w formie zwykłego pisma przy zachowaniu trybu rozstrzygania sporów o właściwość.

Nowe brzmienie nadano również §1 i 2 w art. 73. Określono uprawnienia strony w zakresie dostępu do akt sprawy. Strona ma prawo wglądu w akta sprawy, sporządzania z nich notatek, kopii lub odpisów. Prawo to przysługuje również po zakończeniu postępowania. Jednakże zgodnie z dodanym §1a czynności te mogą być dokonywane w lokalu organu administracji publicznej w obecności pracownika tego organu. Ponadto strona może żądać uwierzytelnienia odpisów lub kopii akt sprawy lub wydania jej z akt sprawy uwierzytelnionych odpisów, o ile jest to uzasadnione ważnym interesem strony. Jednakże uregulowano również formę odmowy stronie dokonywania tychże czynności poprzez zmianę §2 w art. 74, która przewiduję formę postanowienia.

W art. 89 §1 uregulowano tryb przeprowadzenia rozprawy przez organ administracji publicznej. Przeprowadzenie rozprawy w toku postępowania następuje z urzędu lub na wniosek strony.

Art. 101 wprowadza obowiązek zawiadamiania strony o postanowieniu w sprawie zawieszenia albo podjęcia postępowania, a także o przysługujących

jej środkach zaskarżania na postanowienia w sprawie zawieszenia postępowania albo odmowy podjęcia zawieszonego postępowania

Celem nowelizacji art. 105 §1 było wyeliminowanie istniejącej luki prawnej powodującej, że warunkiem umorzenia postępowania jest bezprzedmiotowość całego postępowania. Dzięki tej zmianie organ administracji publicznej będzie mógł umorzyć postępowanie w części, w której stało się ono bezprzedmiotowe, w pozostałym zakresie będzie mógł orzec co do istoty sprawy.

W art. 111 wprowadzono uprawnienie dla organu w zakresie uzupełnienia lub sprostowania decyzji z urzędu Jest to możliwe w terminie 14 dni od dnia doręczenia lub ogłoszenia decyzji.

W art. 126 Kodeksu dopracowano przypadki stosowania przepisów Kodeksu do postanowień.

Nowelizacja art. 138 związana jest z ograniczeniem zbyt częstego korzystania z decyzji kasacyjnych przez organy odwoławcze, w tym celu zawężono możliwość podjęcia decyzji kasacyjnej w stopniu maksymalnym. Ponadto wyeliminowano występujące często sytuacje, w których organ pierwszej instancji wydawał taką samą decyzję, pomimo że wcześniejsza decyzja została uchylona jako wadliwa. Dodano także nową regulacją związaną z wydawaniem decyzji w formie blankietów. Jeżeli przepisy przewidują wydanie decyzji na blankiecie urzędowym, w tym za pomocą środków komunikacji elektronicznej, a istnieją podstawy do zmiany zaskarżonej decyzji, organ odwoławczy uchyla decyzję i zobowiązuje organ pierwszej instancji do wydania decyzji o określonej treści.

Nowelizacja tego przepisu uwzględnia zmiany zawarte w projekcie ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne, ustawy – Kodeks postępowania administracyjnego, ustawy – Ordynacja podatkowa oraz niektórych innych ustaw w zakresie wprowadzenia możliwości doręczania decyzji również za pomocą środków komunikacji elektronicznej.

Zmiana treści art. 149 §1 Kodeksu wynika z dodanego art. 61a, który przesądza, że właściwą formą dla odmowy wszczęcia postępowania w danej sprawie jest postanowienie.

Nowelizacja art. 154 i 155 Kodeksu odebrała organom wyższego stopnia możliwość zmiany ostatecznych decyzji, działającym jako organy pierwszej instancji. Decyzja ostateczna, na mocy której żadna ze stron nie nabyła prawa, może być w każdym czasie uchylona lub zmieniona przez organ administracji publicznej, który ją wydał, jeżeli przemawia za tym interes społeczny lub słuszny interes strony. Decyzja ostateczna, na mocy której strona nabyła prawo, może być w każdym czasie za zgodą strony uchylona lub zmieniona przez organ administracji publicznej, który ją wydał, jeżeli przepisy szczególne nie sprzeciwiają się uchyleniu lub zmianie takiej decyzji i przemawia za tym interes społeczny lub słuszny interes strony.

Nowelizacja art. 229 pkt 2 Kodeksu ma charakter porządkujący. Określa organy uprawnione do rozpatrywania skargi dotyczącej zadań lub wykonywanej działalności w ramach powiatu.

W art. 235 wprowadzono zasadę, że skarga w sprawie, w której była wydana ostateczna decyzja administracyjna, powinna być traktowana jako wniosek o wszczęcie postępowania w jednym z nadzwyczajnych trybów wzruszania decyzji administracyjnych. Organ, do którego taka skarga wpłynie, jest zobowiązany wszcząć postępowanie na wniosek skarżącego, jeżeli jest on stroną lub z urzędu, jeżeli skarga nie będzie pochodziła od strony.

Zmiany w art. 237-239 mają na celu ograniczenie składanych wielokrotnie skarg w tej samej sprawie pomimo tego, że stan faktyczny i prawny tej sprawy nie uległ zmianie, a skarga była już szczegółowo rozpoznana.

W art. 259 określono minimalną częstotliwość dokonywania okresowych ocen przyjmowania i załatwiania skarg i wniosków przez organy i jednostki organizacyjne poddane ich nadzorowi. Ponadto wojewodowie zostali pozbawieni obowiązku dokonywania tych ocen w stosunku do wszystkich organów administracji publicznej i innych jednostek organizacyjnych oraz organizacji społecznych działających na ich terenie.

Kolejną nowelizację w dniu 17 maja 2011 r. wprowadziła ustawa o odpowiedzialności majątkowej funkcjonariuszy publicznych za rażące naruszenie prawa. W art. 37 zmianie uległa treść §2. Organ wyższego stopnia, do którego składane jest zażalenie na niezałatwienie sprawy w terminie, ma uprawnienie do stwierdzenia, czy niezałatwienie sprawy w terminie miało miejsce z rażącym naruszeniem prawa.

Poza ustawami omówionymi powyżej zmiany do Kodeksu postępowania administracyjnego wprowadzają dwie ustawy: ustawa o dowodach osobistych oraz ustawa o ograniczaniu barier administracyjnych dla obywateli i przedsiębiorców. Obie ustawy nowelizują Kodeks na dzień 1 lipca 2011 r. Termin tych zmian nie jest odległy, jednakże 19 maja 2011 r. do Sejmu wpłynął rządowy projekt ustawy zmieniającej ustawę o dowodach osobistych (druk nr 4202). Ustawie tej nadano pilny tryb prac legislacyjnych, gdyż wprowadza ona istotną zmianę w przesunięciu daty wejścia w życie ustawy o dowodach osobistych na dzień 1 stycznia 2013 r. Tym samym ulegnie również przesunięciu data wejście w życie nowelizacji Kodeksu postępowania administracyjnego wynikająca właśnie z ustawy o dowodach osobistych, zatem zmiany te nie będą miały w 2011 roku wpływu na treść Kodeksu postępowania administracyjnego.

Pozostaje jeszcze do omówienia zmiana wynikająca z ustawy o ograniczaniu barier administracyjnych dla obywateli i przedsiębiorców. Z dniem 1 lipca 2011 r. zmieni się brzmienie art. 220 Kodeksu postępowania administracyjnego mającego na celu dostosowanie do systemu składania oświadczeń i zaświadczeń wprowadzonych ustawą o ograniczaniu barier administracyjnych dla obywateli i przedsiębiorców. Organ administracji publicznej nie będzie mógł żądać zaświadczenia ani oświadczenia na potwierdzenie faktów lub stanu prawnego, jeżeli:

1) znane będą one organowi z urzędu,
2) możliwe będą do ustalenia przez organ na podstawie:
   a) posiadanych przez niego ewidencji, rejestrów lub innych danych,
   b) rejestrów publicznych posiadanych przez inne podmioty publiczne, do których organ ma dostęp w drodze elektronicznej na zasadach określonych w przepisach ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne,
   c) wymiany informacji z innym podmiotem publicznym na zasadach określonych w przepisach o informatyzacji działalności podmiotów realizujących zadania publiczne,
   d) przedstawionych przez zainteresowanego do wglądu dokumentów urzędowych (dowodu osobistego, dowodów rejestracyjnych i innych).

Organ administracji publicznej żądający od strony lub innego uczestnika postępowania zaświadczenia albo oświadczenia na potwierdzenie faktów lub stanu prawnego jest obowiązany wskazać przepis prawa wymagający urzędowego potwierdzenia tych faktów lub stanu prawnego w drodze zaświadczenia albo oświadczenia.

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

Są nowe akty wykonawcze do informatyzacji, czyli ePUAP-ką po łapkach

Sebastian Paweł Zalipski

Najgłośniej o informatyzacji administracji publicznej mówiło się chyba w lipcu 2005 r., kiedy wchodziły w życie przepisy ustawy z 20 kwietnia br. o informatyzacji działalności podmiotów realizujących zadania publiczne i nikt tak naprawdę nie miał pojęcia, jakie nowe obowiązki spadną na urzędy i instytucje w całym kraju. Prowadziłem wtedy szkolenia dla przedstawicieli administracji i na własne oczy widziałem, jak wiele było tam obaw i jak często gorączkowo szukano sposobu, by odpowiedzieć na „nowe wyzwania". Parę następnych lat pokazało, że wątpliwości co do „tej całej informatyzacji" pojawiały się nie tylko w podmiotach zobowiązanych do stosowania norm ustawy, ale że miał je również sam ustawodawca, a nawet rozmaite gremia, które wciąż mu pewnie doradzają i wspierają w walce o sukces informatyzacji. Kolejna nowelizacja ustawy, tym razem z roku 2010, odświeżyła tamte obawy i przy pomocy tematu „platformy ePUAP" odświeżyła wątpliwości. Okazało się, że informatyzacja administracji jeszcze nie stała się pustym sloganem wyborczym i najwyraźniej komuś jednak na niej zależy, bo oto światło dzienne ujrzały właśnie rozporządzenia wykonawcze do przepisów o platformie usług administracji publicznej.

Ten nieszczęsny bezpieczny podpis elektroniczny

Nie ma już żadnych powodów, żeby nadal upatrywać w uruchomieniu platformy usług publicznych jakiejś szczególnej rewolucji w normalnej działalności urzędów. Administracja w Polsce już jakiś czas temu otworzyła drzwi przed informatyką i zwykłe użycie komputerów w obsłudze spraw petentów stanowi codzienność polskich urzędów. Przez pewien czas mieliśmy obawy, że udostępnienie Polakom dostępu do urzędów z użyciem przeglądarki w domowym komputerze drastycznie zmieni codzienne obowiązki urzędników. Nie sprawdziły się plany przeniesienia głównego ciężaru obsługi obywateli z korytarzy polskich urzędów na łącza szerokopasmowe. Problemem nie okazał się sam dostęp do Internetu ani też skłonność Polaków do posługiwania się papierem i długopisem zamiast klawiaturą. Internetu używamy wprawdzie coraz częściej, ale raczej do poszukiwania rozrywki, robienia zakupów w sieci czy dodawania nowych wpisów w portalach społecznościowych. Dotarcie do urzędu z wykorzystaniem informatyki sprowadza się dziś praktycznie do spojrzenia na stronę urzędu, odnalezienia godzin urzędowania, miejsca załatwienia danej sprawy albo co najwyżej sprawdzenia czasu oczekiwania w kolejce do obsługi. Potem pokornie zazwyczaj zbieramy potrzebne dokumenty, urywamy się z pracy i wyskakujemy na chwilkę do urzędu w centrum miasta, a szef ze zrozumieniem kiwa głową – „no tak, te cholerne urzędy…". Informatyzacja administracji miała zbudować inną rzeczywistość. Największą przeszkodą dla niej stała się kwestia podpisu elektronicznego, bo jakkolwiek historię tego rozwiązania można już liczyć w dziesiątkach lat (sic!), to w praktyce większości polskich urzędów niełatwo doliczyć się choćby… dziesięciu spraw załatwionych po tym, jak wniosek złożony został za pomocą środka komunikacji elektronicznej opatrzonego podpisem elektronicznym – a dokładniej rzecz biorąc – „*bezpiecznym podpisem elektronicznym weryfikowanym za pomocą kwalifikowanego certyfikatu*". Tenże podpis okazał się, mimo rozmaitych starań, nie tyle

mało sprawnym narzędziem, co fiaskiem marketingowym. Zbyt drogi i ma za mało zastosowań – taka opinia wystarczyła, aby nie mógł dotrzeć w ręce masowego użytkownika. Łatka niepraktycznego, luksusowego gadżetu przywarła już na stałe do tego produktu oferowanego na naszym rynku przez niemających podstaw do zadowolenia dostawców, a ostatecznym gwoździem do trumny podpisu kwalifikowanego stało się upowszechnienie przez urzędy skarbowe możliwości składania deklaracji podatkowych za pomocą sieci i to bez podpisu. Skoro PIT mogę wysłać skarbówce bez „tego wspaniałego e-podpisu”… - więc po co przepłacać?

Zamiast armaty - broń masowego rażenia

Jeśli statystyczny Kowalski ma dziś cokolwiek do załatwienia w urzędzie, to okazja taka zdarza się co najwyżej parę razy do roku i ostatecznie można przeboleć konieczność zorganizowania wolnej chwili na taką okoliczność. Szczerze mówiąc, mało przekonuje myśl, że dla tej odrobiny komfortu i breloczka dopiętego do kluczy warto wspierać budżet któregokolwiek z dostawców elektronicznej sygnatury. Wizerunek podpisu kwalifikowanego cierpi jednak nie przez to, że sprzedaje go jakaś prywatna firma, ale poprzez nadmiernie skomplikowane i zazwyczaj niezrozumiałe zupełnie zasady używania tego narzędzia. Inną sprawą jest, że te komplikacje są niezbędną pochodną wysokiego poziomu bezpieczeństwa, jaki podpis kwalifikowany zapewnia i być może nie da się tego zrobić prościej. Wszystko to sprawia, że podpis kwalifikowany to już nawet nie armata, a bateria rakiet kierowanych wytoczona przeciwko komarowi… Żeby uzyskać w urzędzie zwykłe zaświadczenie, nie potrzeba Kowalskiemu przecież aż takich szerokich gwarancji bezpieczeństwa, a raczej nie codziennie podpisuje on warte miliony umowy przy pomocy e-podpisu. Paradoksalnie tradycyjny sposób obsługi petenta jest znacznie elastyczniejszy, bo bardziej podatny na pewne uchybienia, przymknięcia oka i niedociągnięcia. Nie dawniej niż w zeszłym tygodniu udało mi się wykonać obowiązek meldunkowy za pomocą dokumentu, który wcale nie potwierdzał jednoznacznie moich praw do lokalu. Nie wiem, czy mógłbym liczyć na takie potraktowanie, gdybym wysłał komplet dokumentów drogą elektroniczną urzędnikowi, który spokojnie miałby czas spokojnie je przejrzeć, zamiast kątem oka śledzić kolejkę oczekujących petentów.

Upowszechnienie dostępu do urzędów poprzez Internet miało znacząco wesprzeć upowszechnienie zapowiadanego (ostatnio mniej natarczywie) podpisu dołączanego do nowego dowodu osobistego. Z informacji, jakie mam, wynika, że szanse, aby podpis elektroniczny z dowodem osobistym był udostępniany Polakom, w zapowiadanym terminie są niewielkie. Pewnie pojawi się jednak przed kampanią wyborczą, ale czy będzie to aż taki sukces, jakim nam go wówczas odmalują? Więcej pożytku i to już od zaraz można mieć z elektronicznej Platformy Usług Administracji Publicznej. Co prawda, nowelizacja przepisów jej dotyczących dokonała się w zasadniczej części przed wieloma miesiącami, ale ze względu na brak aktów wykonawczych do ustawy nie można było mówić o realnym wykorzystaniu tego narzędzia.

Idea jest znacznie prostsza niż wykonanie

Na dziś - w olbrzymim uproszczeniu - celem platformy ePUAP jest funkcjonalne połączenie z jednej strony możliwości potwierdzenia swojej tożsamości przez miliony Polaków, a z drugiej dostarczenia im możliwie najobszerniejszego zbioru spraw, jakie mogą chcieć załatwić w urzędach.

Wcale nie trzeba wyrabiać sobie komercyjnego, bezpiecznego podpisu elektronicznego tylko po to, aby raz na jakiś

czas wprowadzić w zdumienie pracownika obsługującego urzędową skrzynkę podawczą. Wystarczy zarejestrować się na platformie, potwierdzić swoją tożsamość w odpowiednim punkcie (tzw. punkcie potwierdzającym) i już. Cóż… trzeba jeszcze mieć nadzieję, że urząd, do którego chcemy się zwrócić, będzie w ogóle obecny na platformie, ale zaraz, zaraz - ustawa o informatyzacji nie wprowadza obowiązkowego zgłoszenia się urzędu ze swoją „ofertą" na ePUAP. Mówi natomiast (dość ogólnie) w art. 16 ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne z dnia 17 lutego 2005 r. (Dz. U. z 20 kwietnia 2005 roku, Nr 64, poz. 565), że podmiot publiczny, organizując przetwarzanie danych w systemie teleinformatycznym, jest obowiązany zapewnić przekazywanie danych również w postaci elektronicznej (przez wymianę dokumentów elektronicznych) m.in. z wykorzystaniem środków komunikacji elektronicznej. Zatem – jeśli masz system w urzędzie, to musi przyjmować e-sprawy. Część urzędów potraktowała to dość poważnie i zainwestowano tam wcale niemałe pieniądze w opracowanie, a potem wdrożenie wielu urządzeń informatycznych. Rozwiązania takie zapewniły urzędom posiadanie przez nich funkcjonalności Elektronicznej Skrzynki Podawczej - ESP i Elektronicznego Potwierdzenia Odbioru - EPO (lub urzędowego potwierdzenia odbioru - UPO). Skoro wystąpiła konieczność przyjmowania dokumentów elektronicznych, zatem nic dziwnego, że chcąc je przyjmować (i potwierdzać złożenie przez petenta), zobowiązany do działania urząd sięgał po rozwiązania dostępne w danej chwili na rynku. Czy te pieniądze zostały zmarnowane i czy wydatkowano publiczne środki na coś, co obecnie można otrzymać w ramach platformy ePUAP za darmo? W pierwszej chwili można tak pomyśleć, ale okazuje się, że nie ma obaw - skoro Kowalski dzięki zaufanemu profilowi będzie mógł już stworzyć dokument i go podpisać, to będzie mógł też złożyć wniosek i wysłać go do właściwego urzędu – nawet jeśli zabraknie go w „menu" ePUAP. Po prostu potwierdzony, uwierzytelniony i rozliczany wniosek wywędruje z platformy do „własnej ESP" odpowiedniego urzędu, a na konto w ePUAP wróci odpowiednie EPO/UPO.

Platforma usług administracji jak e-mail

Korzystanie z ePUAPu będzie przypominało w pewnym stopniu korzystanie z poczty e-mail. Jak niektórzy mogą jeszcze pamiętać, korzystanie z poczty e-mail kiedyś wymagało praktycznie w każdym przypadku posiadania skonfigurowanego programu pocztowego, a dopiero w miarę upływu czasu pojawiły się wygodne (bo już nielimitowane objętościowo) portale pocztowe, dostępne praktycznie z każdego miejsca po zalogowaniu. Korzystanie z programu pocztowego przypominałoby zatem używanie własnego podpisu kwalifikowanego oraz odrębnych dla każdego urzędu rozwiązań ESP/EPO w urzędzie będącym dla petenta adresatem. Kiedy logujemy się do naszego portalu pocztowego, żeby przejrzeć maile i nie chcemy ściągać śmieci na własny komputer, kierujemy się takimi samymi motywami jak te, które sprawią że sięgniemy po ePUAP – wygoda i oszczędność. W ePUAPie mamy swoje quasi-biuro, w którym trzymamy dokumenty, wnioski i gdzie otrzymujemy potwierdzenia odbioru. Wirtualne biuro i wirtualna skrytka pocztowa w jednym. Tyle tylko że jak na razie zadziała wyłącznie na potrzeby naszych kontaktów z administracją - rozwiązanie nie będzie jeszcze na pewno przyjmowane przez organy prowadzące postępowanie karne ani przez sądy cywilne (choć jak słyszałem, zdarzyło się już parę razy, że dokument przesłany przy pomocy formularza z ePUAP został przyjęty w postępowaniu cywilnym - co dowodzi jeszcze wciąż raczej szeroko otwartej głowy Sądu niż popularności platformy w społeczeństwie).

Inną, uciążliwą słabością obecnej konstrukcji platformy jest moim zdaniem wielość różnego typu osób, jakie się w platformie będą pojawiały, mając zgoła odmienne uprawnienia:

- *„Użytkownik”* (bo taką nazwę wprowadza rozporządzenie MSWiA z 27 kwietnia 2011 r. Dz. U. Nr 93 poz. 546) jest osobą fizyczną korzystającą z ePUAP i zakłada na platformie swój własny profil, ma własny identyfikator i hasło.
- Co się tyczy *„podmiotu”*, to może być nim tylko osoba prawna, podmiot publiczny lub jednostka organizacyjna nieposiadająca osobowości prawnej. Podmiot taki ma swój identyfikator i swój własny profil zawierający jego opis, ale jako że *podmiot* sam w swoim imieniu z platformą nic tak naprawdę nie zrobi, to musi mieć też odpowiedniego przedstawiciela - *administratora*.
- *„Administrator”* zakłada konto dla podmiotu i może je również na żądanie podmiotu usunąć. To właśnie jego wskazuje *podmiot* przy składaniu wniosku o udostępnienie danej funkcjonalności platformy, ale administrator nie ma uprawnienia np. do zmiany danych podmiotu – ma je natomiast *użytkownik zarejestrowany.*
- Zmieniać dane zgodnie z literą rozporządzenia ma się zajmować inny typ „usera” platformy: tzw. *„użytkownik zarejestrowany”*. Ta postać to już nie tylko osoba korzystająca z platformy, ale ktoś więcej, bo ww. rozporządzenie określa go już jako „posiadacza konta”. Konia z rzędem temu, kto się w tym nie pogubi… Ciekawe, że *użytkownik zarejestrowany* może działać w imieniu różnych *podmiotów* i akurat to jest dość wygodne, bo np. może występować jako przedstawiciel kilku jednostek organizacyjnych, tworzących też całą osobę prawną, jeśli na platformie zechcą one z jakichś powodów występować osobno (np. uczelnia wyższa ma szereg odrębnych jednostek organizacyjnych - wydziałów).

Dla jasności obrazu warto zerknąć na drugą stronę platformy, gdzie występuje druga grupa uczestników platformy, czyli tzw. *„usługodawcy”*, tj. podmioty publiczne świadczące swoje usługi, załatwiające różnego typu sprawy i obsługujące powierzone im zadania publiczne. Platforma ePUAP pozwala na uzyskanie informacji o podstawie prawnej danej usługi, jej nazwie, odbiorcach i celu, ale także o prawidłowym terminie załatwienia sprawy. Petent, gdy tylko zechce, może zwrócić się o załatwienie danej sprawy do danego urzędu, nie martwiąc się upływającym terminem, zamkniętą pocztą itd., bo już są orzeczenia sądów, które mówią, że „wniesienie pisma uważa się za dokonane w chwili, gdy adresat mógł się z nim zapoznać” – czyli np. o 23:58. Dzięki platformie klient administracji będzie mógł stworzyć właściwy dokument (z użyciem właściwego formularza) i podpisać go przy pomocy czegoś, co rozporządzenie zwie *„zaufanym profilem”* (a który pełni rolę gwarancji ze strony platformy, że osoba podająca się za wnioskodawcę faktycznie nią jest). Autor wniosku może go też od razu wysłać i wnieść stosowną opłatę - jeśli jest wymagana. Także dla urzędu (zwłaszcza tego obecnego na ePUAP) platforma ma szereg pożytków – dzięki niej obsługuje wnioski złożone od uprawnionych osób, prawidłowo podpisane i opłacone, a ponadto przetwarza dokumenty w pełni rozliczalne co do zmian na nich wprowadzonych podczas przetwarzania.

Podmioty świadczące usługi publiczne mogą też w razie potrzeby łączyć swoje „usługi” przy pomocy poszczególnych funkcjonalności platformy i mogą też wymieniać z platformą dane przetwarzane w swoich własnych systemach informatycznych (pod warunkiem otrzymania odpowiedniego certyfikatu bezpieczeństwa – niech żyje interoperacyjność!), w czym wydatnie ma pomagać minister właściwy ds. informatyzacji, a co ww. rozporządzenie precyzyjnie także reguluje.

Jak to powinno być zorganizowane?

Bardziej techniczny charakter ma opis warunków organizacyjnych i technicznych, które ma spełniać system teleinformatyczny służący identyfikacji użytkowników. Został opisany w rozporządzeniu MSWiA z 21 kwietnia 2011 r. (Dz. U. Nr 93 poz. 545). Ten akt wykonawczy w zasadzie stanowi uzupełnienie rozwiązań, których najbardziej brakowało w ustawie o podpisie elektronicznym i opisuje jakie cechy powinien mieć (jakie normy musi spełniać) system zarządzający certyfikacją, tożsamością i autoryzacją użytkowników, ale też podpowiada, gdzie i kiedy publikować „politykę certyfikacji" oraz jak nią zarządzać.

Wreszcie bardzo istotne znaczenie ma także i trzecie rozporządzenie z tej „wykonawczej trójcy", opatrzonej datą 21 kwietnia 2011 r. – rozporządzenie MSWiA w sprawie zasad potwierdzania, przedłużania ważności, wykorzystywania i unieważniania profilu zaufanego platformy ePUAP (Dz. U. Nr 93 poz. 547). Potwierdzenie profilu zaufanego wnioskodawca może osiągnąć w dwóch etapach – w pierwszej kolejności wysyła wniosek (wzór zawarty jest w załączniku do rozporządzenia) w postaci elektronicznej, a następnie w ciągu 14 dni musi udać się do *punktu potwierdzającego*, którego rolę mają pełnić zgodnie z rozporządzeniem: wojewodowie, ZUS, naczelnicy urzędów skarbowych, konsule, a także inne podmioty, o ile wskaże je właściwy w przedmiocie informatyzacji minister. Wojewodowie, naczelnicy i konsule mogą od razu odetchnąć – zadań potwierdzania profilu nie muszą wykonywać osobiście, ale je powierzyć niekaranym za przestępstwo umyślne karne czy skarbowe pracownikom. W punkcie potwierdzającym podstawą do weryfikacji jest dowód osobisty lub paszport, a weryfikuje się oprócz imienia i nazwiska wraz z numerem w zbiorze PESEL także i identyfikator, jaki wnioskodawca sobie założył – powinien go zatem zapamiętać albo odnotować w celu potwierdzenia. Na miejscu wniosek jest drukowany, podpisywany przez wnioskodawcę, a punkt potwierdzający oznacza dodatkowo czas dokonania potwierdzenia i podpisuje profil zaufany odpowiednim podpisem platformy ePUAP albo podpisem certyfikowanym. Do *profilu zaufanego użytkownika* dodane jeszcze będą: identyfikator punktu potwierdzającego, termin ważności profilu (przyznaje się go na 3 lata z możliwością odnawiania na dalsze 3-letnie okresy) oraz oznaczenie sposobu w jaki został podpisany (profil zaufany czy podpis kwalifikowany) . Wszystkie te dane składają się na *„profil zaufany",* którego od tej chwili wnioskodawca używa jako swój własny „podpis". W tym momencie przestaje być on zwykłym użytkownikiem ePUAPu, bo posiadanie własnego *profilu zaufanego* oznacza też i pewne obowiązki. Podobnie jak w przypadku bezpiecznego podpisu certyfikowanego właściciel *profilu zaufanego* ePUAP musi dołożyć wszelkich starań w celu ochrony danych, jakie wykorzystuje, kiedy go używa, nie może udostępniać identyfikatora innym osobom i musi niezwłocznie informować o ewentualnych zmianach czy przeszkodach w używaniu profilu zaufanego (np. o jego utracie). Także i *punkt potwierdzający* ma od tej chwili szereg obowiązków, a najbardziej spektakularny jest chyba obowiązek ministra właściwego ds. informatyzacji przechowywania przez 20 lat dokumentów związanych z potwierdzeniem, przedłużeniem i unieważnianiem *profilu zaufanego*.

Nieprzewidziana (?) korzyść dodana

Prawdziwe spopularyzowanie platformy ePUAP i jej upowszechnienie wśród urzędów będą miały też jeszcze dodatkowy, pozytywny efekt. Minister właściwy do spraw informatyzacji w ramach ePUAP prowadzić ma centralne repozytorium wzorów dokumentów elektronicznych.

Wzory pism, które będą do repozytorium przekazywać poszczególne urzędy, mają powstawać zgodnie z międzynarodowymi standardami dotyczącymi sporządzania dokumentów elektronicznych przez organy administracji publicznej, tj. z uwzględnieniem konieczności podpisywania ich bezpiecznym podpisem elektronicznym. Tymczasem w art. 19b ust. 4 ustawy o informatyzacji dopuszczono wykorzystanie w charakterze *podań* uregulowanych przepisami Kodeksem Postępowania Administracyjnego właśnie takich wzorów, które wpłyną do centralnego repozytorium. Przepis ten stanowi dokładnie, że jeżeli wzór podania określają odrębne przepisy, to umieszczenie wzoru dokumentu elektronicznego przez organy administracji publicznej w centralnym repozytorium jest równoznaczne z określeniem wzoru wnoszenia podań, o których mowa w art. 63 §3a ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego. Ustawa o informatyzacji jest przepisem szczególnym, a zatem rychło powstanie nielichy zbiór wzorów-podań. W ten sposób automatycznie załatwi się problem tworzenia brakujących dotąd dokumentów. Od tej pory zyskają miano obowiązujących w świetle kpa *„formularzy”*.

Administracyjny hipermarket

Przyznam, że do końca maja tego roku dość długo nie zaglądałem na stronę ePUAPu, ponieważ nie mam instynktu testera – tropiciela. Bez przepisów wykonawczych nie było widoków na powodzenie pomysłu platformy usług administracji i bardziej liczyłem już na narzędzia związane z podpisem dodawanym do dowodu osobistego. Jednak po opublikowaniu rozporządzeń poczułem potrzebę przyjrzenia się platformie jeszcze raz i założyłem swój profil. Podzielę się teraz bardzo osobistym odczuciem – podałem wymagane dane, stworzyłem identyfikator, założyłem konto, zalogowałem się i wszedłem… W pierwszej chwili poczułem się jak klient wielkiego centrum handlowego, w którym jednak zamiast butików i sklepów z ceramiką otaczały mnie… urzędy Każdy na wyciągnięcie ręki. Każdy zachęcająco oferuje załatwienie tej czy innej sprawy. Nic tylko przebierać, oglądać i załatwiać. Zaspokoiwszy pierwszy głód, przejrzałem *katalog usług,* szukając właściwego dla mojego miejsca zamieszkania urzędu, w którym zapragnąłem (a co – wolno mi…) złożyć wniosek o zasiłek z tytułu urodzenia dziecka, lecz urzędu tego nie znalazłem. Okazało się, że go tam po prostu nie ma. Kiedy zawiedziony nieco tym, że nie znalazłem w tym „elektronicznym raju petenta” tego, czego faktycznie potrzebowałem – powiedzmy, że przysiadłem na ławce, by zebrać myśli – „co by tu załatwić jeszcze?” Wiem - postanowiłem usunąć numer NIP z mojego konta, który z rozpędu wpisałem w rubryczkę. Widocznie jednak nacisnąłem nie to, co trzeba, bo okazało się, że zniknęło moje konto i kolejna próba zalogowania poskutkowała odmową – choć otrzymałem też informacje, że mój identyfikator jest już zajęty. Irytujące? Nieprawda – po prostu – pojawił się „ochroniarz” i niezadowolonego klienta wywalił z tego przybytku wprost na bruk. Od tej pory nie mam tam wstępu, identyfikator widocznie trafił na „tablicę nieobsługiwanych klientów”, ale innym życzyć będę powodzenia i może trochę więcej szczęścia.

Sebastian Paweł Zalipski - prawnik, dziennikarz, ławnik sądu okręgowego we Wrocławiu, aplikant radcowski. Pracownik Politechniki Wrocławskiej, kieruje Biurem Organizacyjno-Prawnym.

Jaka będzie przyszłość elektronicznej administracji? Część II - perspektywy

Dariusz Bogucki

W poprzedniej części opracowania analizowaliśmy, w jaki sposób zmiany technologiczne oraz otoczenia społeczno-gospodarczego wymuszają ewolucje elektronicznej administracji. Rodzi to nieuniknione pytanie, jak w przyszłości ułożą się losy eGovernment i na próbie odpowiedzi na nie skupimy się w tej części artykułu.

Wyzwania dla sektora publicznego

Wszystkie scenariusze rozwoju eGovernment są zgodne, że sektor publiczny w całej Unii Europejskiej (nie tylko w Polsce) stoi przez historycznymi wyzwaniami.

I. W aspekcie technologicznym

Badacze wiodących światowych think-tanków takich jak IDC czy Rand Corp., a także OECD (*vide „The OECD Technology Outlook 2010"*) są zgodni, że **kluczowym czynnikiem rozwoju krajów staje się umiejętność skutecznego i sprawnego zarządzania wiedzą i wykorzystania technologii informacyjno-komunikacyjnych (ang. skrót ICT).** Wyrazem tego jest wartość światowego rynku IT oszacowana przez IDC w roku 2000 na 984 mld USD. W 2010 r. spodziewana wartość to 1,5 bln USD, co oznacza ponad 50% wzrost w skali 10 lat. A warto dodać, że IDC szacuje ilość wszystkich danych cyfrowych na Ziemi w 2020 r. na **35 ZB (1 ZB = 2^{70} B)**, podczas gdy w 2010 r. było to **0,8 ZB!**

Odnosząc to do administracji, dostrzegamy następujące trendy:

- Rewolucja w obszarze technologii komunikacyjnych i informacyjnych (ICT), której rezultatem był dynamiczny rozwój rozwiązań elektronicznego biznesu i elektronicznej bankowości, wymusza stosowanie takich samych metod i form świadczenia usług przez administrację. A warto przypomnieć, że inicjatywa kluczowa „Unia Innowacji" zakłada pełnienie przez administrację roli stymulatora innowacyjnych zmian.
- Nowe formy świadczenia usług wykorzystujących owoce kolejnej fali rewolucyjnego wzrostu technologicznego konsumujące wejście do powszechnej eksploatacji technologii szerokopasmowej transmisji danych, jak m.in. telefonia mobilna 4G, sieci NGN/NGA czy cyfrowy przekaz radiowy i telewizyjny. Sceptykom wystarczy przypomnieć, że aplikacje na urządzenia mobilne jeszcze kilka lat temu były ciekawostką, a obecnie IDC szacuje, że do 2014 r. średnioroczna stopa wzrostu rozwiązań dla urządzeń mobilnych wyniesie 18,4%. Warto dodać, że na 2015 r. Rand przewiduje wejście do użytku nowej klasy urządzeń mobilnych wykorzystujących np. możliwości elastycznych wyświetlaczy OLED.
- Następuje przewartościowanie roli komponentów systemów teleinformacyjnych: rola infrastruktury minimalizuje się na rzecz outsourcingu mocy obliczeniowych, czego implementacją jest tzw. cloud computing. Najnowszy (za rok 2010) raport IDC przewiduje, że rynek oprogramowania dostępnego „z chmury" zwiększy się do 2014 r. o ponad 25%. W 2020 r. w miejsce tradycyjnego zakupu licencji i opieki serwisowej uiszczanej corocznie organizacje będą uiszczać opłaty subskrypcyjne, zależne od stopnia wykorzystania

oprogramowania. Jest to także wynik coraz powszechniejszego zastosowania rozwiązań budowanych w oparciu o model OSS (tj. Otwartego Oprogramowania).

Tym samym zakup dostępu do aplikacji w coraz mniejszym stopniu będzie obciążał budżety inwestycyjne, a coraz bardziej operacyjne, co radykalnie zmieni sposób funkcjonowania służb informatycznych administracji. Zamiast budować system można będzie z niego skorzystać jak z usługi dostępnej przez Sieć. W rezultacie własność danych zastąpi dotychczasową własność systemu informatycznego. Takie podejście będzie stawiało zarówno przed dostawcami, jak i przed użytkownikami nowe wyzwania związane przede wszystkim z kwestiami dobrego zrozumienia potrzeb i umiejętności ich zdefiniowania.

II. W aspekcie społeczno-ekonomicznym

- Konsekwencje zmian demograficznych:
  - Postępujące starzenie się społeczeństw krajów unijnych.
    Ludność Europy starzeje się w szybkim tempie: średnia długość życia Europejczyka zwiększyła się z 55 lat w 1920 r. do 80 lat obecnie. Prognozy demograficzne dla krajów EU-27 wskazują, że w latach 2010–2030 wraz z przechodzeniem na emeryturę pokolenia wyżu demograficznego liczność grupy osób powyżej 65 lat wzrośnie prawie o 40%, by w 2050 roku stanowić ok. 30% populacji. Stanowi to ogromne wyzwanie dla społeczeństw i gospodarek krajów nie tylko UE.
  - Skutki procesu migracji.
    Pozytywne skutki imigracji, zwłaszcza w kontekście opisanego procesu starzenia się społeczeństwa europejskiego, wymagać będą znacznie skuteczniejszych niż to było dotychczas działań integracyjnych oraz środków ochrony przed napływem osób niepożądanych, a więc sprawnych i skutecznych działań w obydwu obszarach.
- Państwo (administracja) już obecnie coraz częściej musiało sprawować swoje funkcje wobec obywateli fizycznie rozrzuconych po całym terytorium UE (a może i świecie), co praktycznie przekłada się na to, że administracja będzie funkcjonować w aspekcie transgranicznym w trybie 7/24. Przypomnijmy, że u fundamentów omawianego w poprzedniej części paradygmatu zarządzania wartością publiczną (PVM) leżała właśnie próba obiektywnej oceny usług administracji publicznej w aspekcie modernizacji zgodnie z potrzebami społecznymi.
- Wzrastająca mobilność społeczeństw europejskich, skutkująca tym, że administracje wszystkich państw członkowskich Unii Europejskich muszą zmierzyć się z problemem funkcjonowania w wielojęzycznym i wielokulturowym środowisku.
- Aplikacje tzw. Web 2.0/3.0 dowodzą praktycznie tezy prof. Manuela Castellsa, że w społeczeństwie wykorzystującym aktywnie nowoczesne technologie, komunikującym się za pośrednictwem globalnej sieci, wymiana poglądów następuje w sposób niezwykle sprawny i skuteczny. Łańcuch komunikacji będzie mógł zatem w sposób nieograniczony być rozszerzany o nowych uczestników procesu.
- Rosnąca mobilność społeczeństw UE wynikająca z coraz pełniejszego wykorzystaniem możliwości, jakie niesie jednolity rynek wewnętrzny UE.
- Przesuwanie się (a historycznie rzecz ujmując, powrót) centrum rozwoju gospodarczego świata do Azji. Ekonomiści przewidują, że w horyzoncie 2020 roku największymi gospodarkami światowymi będą, jak do XVI wieku, Chiny i Indie.

III. W aspekcie organizacyjno-prawnym

- Opracowania Europejskiego Instytutu Administracji Publicznej (EIPA) wskazują, że model funkcjonowania administracji krajów UE wymaga rewizji: nowe rozwiązania technologiczne umożliwiają wszak bezpośrednie i aktywne uczestnictwo obywateli w procesie zarządzania państwem i bezpośredni nadzór nad poczynaniami urzędników.
- Niezbędne jest dopasowanie administracji do nowych trendów w zatrudnieniu: upowszechniająca się telepraca i przejście z pracy na całe życie do wielozawodowości, a nade wszystko upowszechniający się w krajach „starej Unii" proces zstępowania tradycyjnego modelu służby cywilnej systemem kontraktów specjalistycznych i menedżerskich.
- W tym kontekście należy spodziewać się, że obecny układ sektorowy administracji (nie tylko polskiej) będzie stopniowo zastępowany strukturą projektową o charakterze macierzowym.

Scenariusze rozwoju eGovernment

W kontekście opisanych wyżej przemian oczywiste jest, że powstać muszą rozwiązania prawne i organizacyjne umożliwiające zmianę sposobu zarządzania państwem (governance). W tym kontekście pojawia się nieuniknione pytanie o przyszłą rolę eGovernment w tym procesie.

W ostatnim czasie powstało szereg opracowań kreślących możliwe scenariusze rozwoju, ale jak się wydaje najpełniejsza analizę przedstawiają wspomniane w poprzedniej części opracowania raporty szwedzkiej Agencji Innowacji w Administracji Vinnowa (Vinnowa Report VR 2006: 11 „*The future of eGovernment, Scenarios 2016*" oraz Vinnova Report VR 2009: 28 *„eGovernment of Tomorrow, Future Scenarios for 2020").* Warto im przyjrzeć się dokładniej, bo to wnioski z tych raportów były ważnym przyczynkiem do prac Komisji Europejskiej nad inicjatywami kluczowymi „Europejska Agenda Cyfrowa" i „Unia Innowacji".

Analizując wspomniane wnioski, musimy pamiętać, że mówiąc o scenariuszu rozwoju jakiejś sytuacji, kreślimy jedynie pewien model możliwych zdarzeń w przyszłości. Scenariusz pokazuje jedynie, w którym kierunku sytuacja może się zmienić i pod jakimi warunkami. Zdaniem Vinnowa takimi dwoma najbardziej krytycznymi czynnikami o największym stopniu oddziaływania, a zarazem o największej niepewności, będą w przyszłości następujące zmienne:

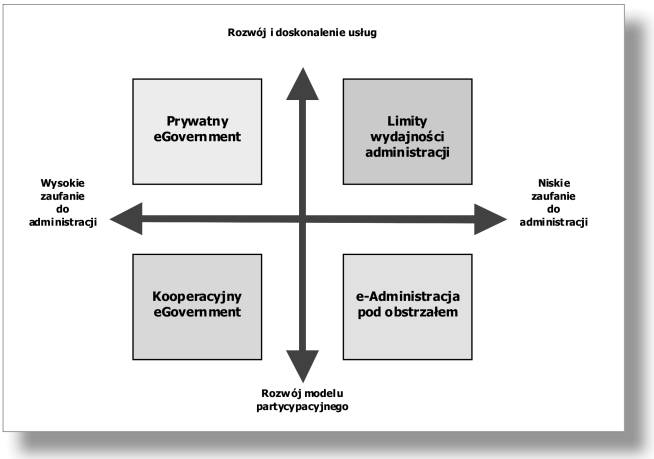
- **Jak kształtować się będzie wzajemne zaufanie obywateli (i firm) i administracji?**

Czy w przyszłości administracja publiczna nadal będzie pełnić rolę swoistej zaufanej strony dla obywateli i firm i obejmować swoim nadzorem kolejne obszary aktywności (wysokie zaufanie do administracji), czy też stopniowo będzie wypierana przez postępującą samoorganizację społeczeństwa na bazie rozbudowanych interakcji sieciowych (niskie zaufanie do administracji)?

- **Jaki model funkcjonowania przyjmie administracja?**

Czy kontakt administracji z obywatelami/firmami będzie zmierzać w stronę modelu partycypacyjnego, opartego o przedstawicielski model zarządzania Państwem (governance) z wykorzystaniem metod pracy zespołowej i wiedzy wszystkich zaangażowanych stron (w tym mediów, organizacji pozarządowych i opozycji), czy na zaspakajaniu rosnącego popytu na nowe i rozwijane usługi elektroniczne?

Te zmienne tworzą cztery możliwe scenariusze (patrz: rysunek 1).



Rysunek 1

- **Scenariusz „Prywatnego eGovernment"** zakłada, że popyt na usługi elektroniczne będzie rósł lawinowo, stanowiąc coraz większe obciążenie dla Państwa. Dlatego też bazując na dobrym kontakcie z użytkownikami, administracja może zdecydować się na ograniczenie inwestycji w warstwę aplikacyjną i przeniesienie na podmioty komercyjne ciężaru rozwoju usług (w formie partnerstwa publiczno-prywatnego lub analogicznej).
  W polskich warunkach scenariusz ten wydaje się abstrakcyjny, zwłaszcza w świetle bardzo ograniczonych działań bazujących na partnerstwie publiczno-prywatnym. Jednak w innych krajach, zwłaszcza w USA, takie rozwiązanie jest poważnie analizowane, by wspomnieć tylko USA i administrację prezydenta Obamy, która prowadzi w kilku departamentach takie publiczno-prywatne pilotaże.
- **Scenariusz „Limitów wydajności administracji"** jest podobny do poprzedniego z tą różnicą, że administracja pozostawia całkowicie w swojej domenie rozwój usług elektronicznych. Jest to zatem model, w jakim odbywał się rozwój usług e-Government na początku ich wprowadzania. Praktyka pokazuje, że jest on także kosztowny w realizacji, dlatego że rozwój tak „odgórnie planowanych usług" nie nadąża za szybko rosnącymi potrzebami użytkowników (stąd nazwa modelu).
- **Scenariusz „e-Administracja pod obstrzałem"**: administracja działająca „odgórnie" nie potrafi/nie chce zbudować efektywnych kanałów komunikacyjnych ze społeczeństwem. Z drugiej strony społeczeństwo stworzyło świetnie funkcjonujące kanały komunikacji. Po drugiej strony urzędowej lady stoi zatem nie pojedynczy klient, a świetnie doinformowana, znająca swoje prawa grupa użytkowników, pod której obstrzałem znajduje się administracja. Nie jest to zatem scenariusz optymistyczny dla administracji.
- **Scenariusz „kooperacyjny eGovernment"** zakłada aktywny udział administracji w tworzeniu społecznościowych kanałów komunikacji ze społeczeństwem, które zastępują/uzupełniają tradycyjne usługi elektroniczne. Jak się wydaje, jest to scenariusz najbardziej nieokreślony, albowiem bardzo głębokiej redefinicji ulegnie dotychczasowy model zarządzania państwem, a zwłaszcza rozumienie takich pojęć jak neutralność polityczna, opozycyjność i rządy prawa.

Dokąd zmierzasz polska elektroniczna administracjo?

Warto przypomnieć, że podobne scenariusze nakreślił w roku 2008 Narodowy Program Foresight Polska 2020 w polu badawczym „Technologie informacyjne i komunikacyjne".

Wyniki prac tzw. panelu głównego wskazują jednoznacznie, że w świetle opisanych w niniejszym artykule trendów społeczno-ekonomicznych, technologicznych i organizacyjno-prawnych, dotychczasowy model zastosowania technologii ICT w jednostkach administracji nie przynosi oczekiwanych efektów. Działalność ta sprowadzała się bowiem do wdrażania kolejnych niepowiązanych ze sobą systemów informatycznych. Ich niezbędności dla funkcjonowania Państwa nikt oczywiście nie neguje, tym niemniej budowanie ich jako niezależne silosy informacyjne nie mogło przynieść zawierzanych efektów. Znane są wszak przypadki, kiedy to politycy i parlamentarzyści – albo lekceważąc znaczenie teleinformatyki w usprawnianiu organizacji i zarządzania państwem albo tego znaczenia nie rozumiejąc – stanowili prawo, które utrudniało skuteczne wykorzystanie teleinformatyki do wsparcia administracji publicznej.

Program Foresight Polska 2020 nakreślił 2 skrajne scenariusze:

- **Kontynuacja obecnego sposobu „informatyzacji administracji",** co skutkuje następująco:
  - **Informatyzacja administracji publicznej nie odnosi się do kluczowej kwestii, jaką jest sprawniejsze zarządzanie państwem z wykorzystaniem systemowych i technicznych narzędzi teleinformatyki.** Dlatego też polska administracja pozostaje nadal niewydolna, kosztowna i anachroniczna pod względem struktury. Tchórzostwo elit politycznych nie pozwala na żadne gruntowne zmiany w sposobie zarządzania państwem. Administracja jest przez to immanentnie niezdolna do prowadzenia planowych działań.
  - Administracja nie jest zainteresowana wdrażaniem rozwiązań innowacyjnych, zwłaszcza w zakresie szerszego stosowania w zarządzaniu technologii informacyjnych. Dominuje działanie reaktywne i wymuszone w stylu dziewiętnastowiecznych carskich czynowników.
  - Systemy informatyczne są archaiczne i informatyzują tradycyjne funkcje. Administracja nadal tworzy „informatykę silosową" – każdy resort buduje swój własny, autonomiczny system. Brak jest zarządzania portfelem projektów w administracji państwowej. Dominuje wymiana papierowa informacji. Administracji wciąż brakuje kadr do zajmowania się nowymi zagadnieniami.
  - Brakuje mechanizmów doskonalenia zawodowego administracji. W konsekwencji postępuje negatywna selekcja i duża rotacja kadr. Praca w administracji nie jest atrakcyjna dla młodych, perspektywicznych osób (chyba że jako element zdobycia praktyki). Ci, co mają już doświadczenie i stosowne kompetencje, trafiają do biznesu i organizacji pozarządowych albo wyjeżdżają za granicę.

Odnosząc to do modelu Vinnowa, jest to połączenie scenariuszy tzw. niskiego zaufania, tj. „e-Administracja pod obstrzałem" i „Limity wydajności administracji".

- **Wykorzystanie rozwiązań teleinformatycznych do usprawnienia zarządzania państwem,** które niejako sumuje modele „wysokiego zaufania do administracji" Vinnowa:
  - Wyposażona w sprawne systemy informacyjne polska administracja jest ważnym czynnikiem budowy kapitału intelektualnego kraju.
  - Systemy informacyjne budowane są w ścisłej współpracy z użytkownikami końcowymi. Państwo ufa swojemu obywatelowi i zgadza się, żeby ten udostępniał samodzielnie swoje dane osobowe, dokumenty i inne ważne dla niego treści.
  - Bazy wiedzy administracji pozwalają na skuteczne zarządzanie projektami o wymiarze państwowym. Ściśle z nimi

współdziałają współpracujące ze sobą systemy informacyjne administracji – zwłaszcza administracji lokalnej (samorządowej), bezpośrednio obsługujące obywateli i przedsiębiorców, nakierowane na ich konkretne potrzeby.

- Administracja jest niewielka i sprawna. Wymaganie wysokich kwalifikacji, stałe mechanizmy doskonalenia kwalifikacji powodują, że praca w administracji jest wyróżnieniem i prestiżem. Dzięki temu administracja planuje i podejmuje aktywne i skuteczne działania nakierowane na aktywizację konkretnych grup, np. seniorów, młodzieży, integrację emigrantów itd. Aktywnie stymuluje wdrażanie rozwiązań innowacyjnych, ściśle współdziała z ośrodkami naukowymi i rozwojowymi.

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

Polecamy

Cyfrowe biuro

ABBYY FineReader –przekształcanie skanów i plików PDF na format edytowalny

Kiedy warto stosować?

Każdego dnia do urzędów, instytucji, kancelarii spływają tysiące drukowanych dokumentów papierowych, elektronicznych i faksów. Wszystkie te dokumenty są gromadzone w archiwach papierowych lub elektronicznych. Znalezienie potrzebnego dokumentu w tych zasobach wymaga czasu. Aby można je było łatwo i szybko wyszukać w archiwum elektronicznym, należy poddać strony procesowi OCR (Optical Character Recognition) i zapisać w formacie edytowalnym, przeszukiwanym, np. PDF/a. Służy do tego program ABBYY FineReader, który jest często implementowany w systemach typu DMS (Document Management System).

Jakie są inne zastosowania?

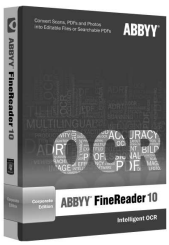
Program ABBYY FineReader używany jest również do automatycznego przekształcania skanów i plików PDF do postaci edytowalnej. Pozwala wyeliminować ręczne przepisywanie faksów czy dokumentów papierowych oraz zwiększa efektywność i ułatwia pracę biurową.

Wystarczy skaner (urządzenie sieciowe skanujące), komputer i oprogramowanie ABBYY FineReader. Program ABBYY FineReader przekształca zeskanowane strony drukowane na postać edytowalną np. Worda czy Excela. Robi to 100 razy szybciej niż profesjonalna maszynistka. Zachowuje kształt i wielkość czcionek, tabele, nagłówki, stopki i hiperłącza. A co ważne, program jest prosty w obsłudze, a także dostępny w polskiej wersji. Dla porównania ręczne wprowadzenie dokumentu A4 do komputera zajmuje około 20 minut. Z FineReaderem można to zrobić w ciągu około minuty.

Jeśli w biurze wprowadzany jest często lub sporadycznie tekst z papieru do komputera, warto pomyśleć o programie OCR.

Ponieważ użytkownik stale nie korzysta z programu ABBYY FineReader, producent wprowadził sieciowe licencjonowanie jednoczesne. Program w wersji Corporate Edition można zainstalować na dowolnej ilości komputerów w sieci, a z programu może korzystać w danym momencie tyle osób, ile licencji urząd/instytucja/kancelaria posiada. Koszt jednej licencji wynosi około 1000 zł netto.

Zobacz i przetestuj bezpłatnie,
jak działa program: **www.finereader.pl.**



Czy Europa potrzebuje strategii cyfrowej?

Edyta Marcinkowska

Współczesne zmiany w technologiach informacyjno-komunikacyjnych są tak samo rewolucyjne jak rozwój sieci elektrycznych i transportowych u progu XX wieku. Skoro bez elektryczności i transportu nie byłoby rewolucji industrialnej, wyobraźmy sobie, jakie zamiany w gospodarce oraz życiu społecznym Polaków wywoła stosowanie technologii cyfrowych.

***C**hociaż dla wielu Europejczyków „cyfrowe życie" oparte o ogólnoświatową technologię o nieograniczonym zasięgu staje się rzeczywistością, to nie mogą oni pogodzić się z faktem, że wspólny rynek opracowany przed powstaniem Internetu pozostaje bardzo niekompletny w sferze wirtualnej* – czytamy we wprowadzeniu do Europejskiej Agendy Cyfrowej na lata 2010-2020. Obawy Europejczyków związane z niewystarczającym dostępem do Sieci, opieszałością w budowie szerokopasmowych łączy internetowych, zagwarantowaniem prywatności i bezpieczeństwa użytkowania sieci WWW, a także – o czym nie należy zapominać – brakiem kompetencji w zakresie obsługi komputera wydają się być uzasadnione, gdy przywołamy liczby. Wynika z nich jasno, że Europa pozostaje w tyle za swoimi partnerami przemysłowymi – USA i Japonią.

Dane wskazują, że około „30% Europejczyków nigdy nie korzystało z Internetu. Liczba pobieranych plików muzycznych jest cztery razy wyższa w USA niż w UE z uwagi na brak legalnych ofert i fragmentację rynków. (…) jedynie 1% Europejczyków ma dostęp do szybkich sieci światłowodowych w porównaniu z 12% Japończyków i 15% mieszkańców Korei Południowej. Wydatki UE na badania i rozwój w dziedzinie technologii informacyjno-komunikacyjnych stanowią tylko 40% poziomu wydatków USA na te cele". Z takimi wynikami Europa nie jest w stanie odnieść sukcesu w dynamicznie rozwijającym się sektorze gospodarki opartym na wiedzy. Potrzebuje spójnego planu działania na rzecz jak najlepszego wykorzystania technologii informacyjno-komunikacyjnych (dalej: ICT) w celu przyspieszenia naprawy gospodarczej i stworzenia podstaw zrównoważonej przyszłości cyfrowej UE. Rolę tę pełni Europejska Agenda Cyfrowa (dalej: agenda).

Komisja Europejska przyjęła agendę 19 maja 2010 r. Oficjalnej jej prezentacji dokonała wiceprzewodnicząca Komisji Europejskiej i Komisarz ds. Agendy Cyfrowej, Neelie Kroes, 31 maja 2010 r. w Brukseli w trakcie posiedzenia Rady UE do spraw Transportu, Telekomunikacji i Energii. Dokument ten jest pierwszą z siedmiu flagowych inicjatyw Strategii UE 2020. Dziesięcioletni okres realizacji agendy ma przyczynić się do uzyskania trwałych korzyści ekonomicznych i społecznych z jednolitego rynku cyfrowego. Agenda, podobnie jak poprzedzająca ją inicjatywa i2010, jest dokumentem strategicznym i zawiera około stu działań o charakterze legislacyjnym i pozalegislacyjnym w obszarze społeczeństwa informacyjnego.

Strategia użyteczna

Celem agendy jest nakreślenie drogi pozwalającej na maksymalne wykorzystanie ekonomicznego i społecznego potencjału ICT, w szczególności Internetu, który stanowi ważny środek działalności gospodarczej i społecznej: służy on pracy, zabawie, komunikacji oraz pozwala na swobodne wyrażanie poglądów. Sukces agendy przyczyni się do wzrostu innowacyjności, wzrostu gospodarczego oraz poprawy codziennego życia obywateli i przedsiębiorców. Szersze i skuteczniejsze zastosowanie technologii cyfrowych umożliwi Europie zmierzenie się z głównymi stojącymi przed nią wyzwaniami.

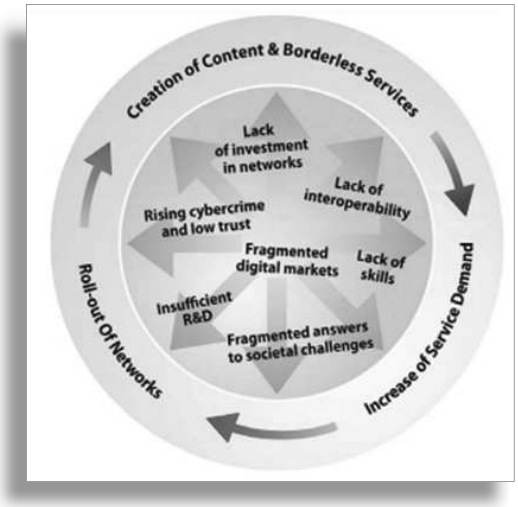
Pracom nad agendą przyświecała wizja stworzenia strategii użytecznej, pozwalającej na uzyskanie trwałych korzyści ekonomicznych i społecznych z funkcjonowania jednolitego rynku cyfrowego, którego podstawą mają być bardzo szybki Internet oraz interoperacyjne aplikacje. Agenda jest dokumentem odwołującym się do rzeczywistych potrzeb. Przy jej tworzeniu brano pod uwagę kluczowe dokumenty, a wśród nich: Sprawozdanie w sprawie konkurencyjności Europy w dziedzinie technologii cyfrowych (COM (2009) 390), Konsultacje Komisji z 2009 r. dotyczące przyszłych priorytetów ICT, Konkluzje rady ds. TTE z grudnia 2009 r., Strategię Europa 2020, Konsultacje w sprawie tej strategii, Wkład partnerstwa branży ICT w strategię „Cyfrowa Europa" prezydencji hiszpańskiej, Sprawozdanie Parlamentu Europejskiego z własnej inicjatywy dotyczące 2015.eu, Deklarację uzgodnieniową podczas nieoficjalnego spotkania ministrów w Grenadzie w kwietniu 2010 r.)[1]. Pogłębiona analiza potrzeb oraz Strategia Europa 2020 – jako dokument nadrzędny – sprawiają, że agenda stanowi kompleksowy plan rozwoju sektora ICT oraz telekomunikacji na terenie Unii Europejskiej do roku 2020 r.

Monopolista – Internet

Agenda ma przygotować unijną gospodarkę na wyzwania następnego dziesięciolecia. Obecnie „(…) sektor ICT odpowiada bezpośrednio za 5% europejskiego PKB, a jego wartość rynkowa wynosi 660 mld EUR rocznie, jednakże o wiele bardziej przyczynia się on do ogólnego wzrostu produktywności (20% bezpośrednio z sektora ICT, a 30% z inwestycji w ICT." Taki stan rzeczy wynika z innowacyjnego charakteru tego sektora oraz właściwej mu dynamiki. Wszelkie przesłanki pozwalają przypuszczać, że w przyszłości sektor ICT będzie generował znaczną wartość PKB.

Przewiduje się, że do 2020 roku treści i aplikacje cyfrowe będą udostępniane i dostarczane niemalże wyłącznie za pośrednictwem Internetu. Dlatego wystarczy udostępnić atrakcyjne zbiory w równie atrakcyjnym, interoperacyjnym i eksterytorialnym, środowisku internetowym. Chęć obcowania z takimi treściami pobudzi z kolei popyt na większą szybkość i przepustowość łączy internetowych. Stale rosnące zapotrzebowanie na sprawny Internet uzasadni inwestycje w szybsze łącza internetowe. Zaś upowszechnienie nowoczesnych sieci otworzy drogę kolejnym innowacyjnym usługom. W ten sposób powstaje samonapędzający się proces gospodarki cyfrowej, w którym ICT będą stymulowały gospodarkę UE.

1 Dokumenty te znaleźć można na stronie: http://tinyurl.com/2rxcb2.



Rys. 1.: Samonapędzający się proces gospodarki cyfrowej
za: Europejska Agenda Cyfrowa (PL) 2010, s. 5.

Na zewnątrz: tworzenie eksterytorialnych serwisów i treści, wzrost dostępności usług, zwiększanie przepustowości sieci.

Wewnątrz: podzielony rynek cyfrowy, brak interoperacyjności, wzrost cyberprzestępczości i spadek zaufania do Sieci, brak inwestycji w Sieci, niewystarczające nakłady na badania i innowacje, brak umiejętności wykorzystywania technologii cyfrowych, niewykorzystane możliwości w zakresie sprostania wyzwaniom społecznym.

Poważnie i konsekwentnie

Rozwój usług transgranicznych stanie się nieosiągalny, jeśli w możliwie jak najszybszym czasie nie zostaną uporządkowane kwestie związane m. in. z ochroną praw autorskich twórców, ze spójnym system ochrony konsumentów oraz z ochroną danych osobowych. Dlatego agenda organizuje główne działania wokół potrzeby systemowego rozwiązania siedmiu obszarów problemowych:

1. Ujednolicenie rynku internetowego handlu i usług poprzez uproszczenie praw autorskich, licencji transgranicznych oraz wprowadzenie ułatwień w dziedzinie płatności elektronicznych i fakturowania.
2. Poprawa w dziedzinach otwartości standardów i interoperacyjności w usługach ICT, by wzmóc rozwój innowacyjności i kreatywności.
3. Wzrost zaufania i bezpieczeństwa w sieci poprzez ochronę danych osobowych oraz skuteczne przeciwdziałanie atakom cybernetycznym.
4. Zapewnienie dostępu do szybkiego Internetu poprzez docelowe udostępnienie każdemu obywatelowi państw UE dostępu do Internetu o szybkości 30 Mb/s, a dla co najmniej połowy gospodarstw domowych – 100 Mb/s (do roku 2020) oraz poprzez stworzenie korzystnych warunków dla inwestycji w łącza szerokopasmowe i sieci światłowodowe.
5. Pobudzanie innowacji i badań w dziedzinie ICT poprzez wzrost nakładów na badania i wspieranie inwestycji za pośrednictwem funduszy regionalnych.
6. Zapewnienie wszystkim obywatelom niezbędnej wiedzy i umiejętności, by mogli niezależnie od statusu społecznego korzystać z usług internetowych (w tym usług handlowych, zdrowotnych, edukacyjnych i socjalnych).
7. Uwolnienie społecznego potencjału ICT i jego wykorzystanie do pomocy osobom starszym, niepełnosprawnym,

wymagającym opieki zdrowotnej poprzez np. powszechny dostęp do danych medycznych oraz dla poprawy jakości środowiska naturalnego.

Uporządkowanie prawodawstwa w obszarze cyfrowych usług na terenie Unii Europejskiej oraz walka z negatywnymi zjawiskami społecznymi i gospodarczymi, w tym z wykluczeniem cyfrowym, wymaga przyjęcia odpowiedzialności na najwyższym szczeblu politycznym i dowodzi, że agenda jest Europie potrzebna. Jest niezbędnym, ale także ambitnym planem działania na najbliższe lata. Określa siedem priorytetowych obszarów, w ramach których zostanie podjętych około stu działań, z czego trzydzieści jeden będzie miało charakter legislacyjny. Rozwój i ewolucja tej inicjatywy – w formie projektu przewodniego strategii Europa 2020 – przewidziano na lata 2010-2020.

Aby w pełni zrealizować program Europejskiej Agendy Cyfrowej, Komisja Europejska będzie ściśle współpracowała z Parlamentem Europejskim, państwami członkowskimi oraz ze wszystkimi zainteresowanymi stronami. Komisja utworzy ukierunkowane na działania platformy z udziałem zainteresowanych stron, a także będzie organizować coroczne zgromadzenia cyfrowe w celu oceny postępów i nowych wyzwań.

Źródło: Europejska Agenda Cyfrowa (PL) 2010.

Edyta Marcinkowska - w latach 2009-2010 związana z Ministerstwem Spraw Wewnętrznych i Administracji. Zajmuje się problematyką społeczeństwa informacyjnego.

Proponujemy

SEMINARIUM
„BIBLIOTEKI CYFROWE A PRAWO AUTORSKIE"
21 lipca 2011 r., Warszawa

W PROGRAMIE:

- Procedury prawne i organizacyjne tworzenia bibliotek cyfrowych. Obszary ryzyka w procesach budowania bibliotek cyfrowych.
  Barbara Szczepańska (Kancelaria Prawna Hogan Lovells)
- Prawo autorskie a biblioteki cyfrowe. Legalność bibliotek cyfrowych - odpowiedzialność cywilno-prawna z tytułu naruszeń praw autorskich.
  dr Sybilla Stanisławska-Kloc (Uniwersytet Jagielloński, Instytut Prawa Własności Intelektualnej)
- E-booki, audio-booki, płyty CD i DVD - aspekty prawne nowych technologii w bibliotekach cyfrowych i zasady z ich korzystania. Nowe pojęcia technologiczne w kontekście bibliotek cyfrowych.
  Adwokat Piotr Łada

Więcej: www.cpi.com.pl

cpi
centrum promocji informatyki

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

Wojciech Kaliński

Rekomendacja nr 3: Konstruowanie zamówienia z uwzględnieniem cyklu życia systemu

Wśród typowych błędów związanych z przedmiotową rekomendacją Urząd Zamówień Publicznych wskazuje na następujące problemy:

Zamówienie sprzętu bez obsługi serwisowej, niezbędnej do jego niezawodnego funkcjonowania w przewidzianym okresie eksploatacji. Konsekwencją tego spostrzeżenia jest zalecenie, by SIWZ i umowa dla zamówień na sprzęt informatyczny obejmowały nie tylko dostawę sprzętu, ale także usługi serwisu i konserwacji sprzętu niezbędnych do osiągnięcia i utrzymania jego wymaganej niezawodności i wydajności w całym planowanym okresie eksploatacji, a więc usługi świadczone w okresie eksploatacji.

Rzeczywiście należy zgodzić się tezą, że sam zakup sprzętu bez jego obsługi serwisowej jest niewystarczający. Zwłaszcza, że warunki gwarancyjne są w większości przypadków wysoce niezadowalające i niewystarczające dla zapewnienia odpowiedniego poziomu serwisu. Oczywiście w praktyce niezwykle rzadko zdarza się tak, że w przypadku serwisu sprzętu Zamawiający będzie zdany wyłącznie na jednego wykonawcę. Poza przypadkami serwisu producenckiego każdy producent ma wielu partnerów serwisowych, którzy mogą taką usługę świadczyć i którzy mogą wziąć udział w konkurencyjnym przetargu. Analizując objęcie zakupu sprzętu i jego serwisowania jednym postępowaniem albo w oddzielnych przetargach, warto zwrócić uwagę na warunki oferowanej gwarancji. Może się bowiem okazać, że przekazanie serwisowania w ręce nawet innego partnera danego producenta skutkować będzie utratą gwarancji. Tymczasem postępowanie równolegle w sprawie uprawnień gwarancyjnych i serwisowych daje Zamawiającemu dwojakiego rodzaju korzyści. Po pierwsze, w przypadku gdy inna firma jest gwarantem, a inna podmiotem serwisującym, w razie niewykonania serwisu istnieje możliwość zwrócenia się do innego podmiotu na podstawie gwarancji. Ponadto w razie, gdyby doszło do rozwiązania (wypowiedzenia) umowy serwisowej, Zamawiającemu pozostaną jeszcze uprawnienia z tytułu gwarancji. Gdyby jednak warunki gwarancyjne nie dopuszczały możliwości świadczenia serwisu przez inny podmiot niż gwarant, nawet jeśli jest on autoryzowanym serwisem producenta, za wskazane należy uznać objęcie jednym przetargiem zarówno zakupu sprzętu, jak i jego serwisu tak, by następnie Zamawiający nie stał pod ścianą na skutek monopolistycznej w tym zakresie pozycji danego Wykonawcy.

Oczywiście wadą łączenia zakupu sprzętu i serwisu w jednym postępowaniu jest konieczność zapewniania sobie środków na oba elementy umowy. Ponadto dostawy będę realizowane co do zasady ze środków inwestycyjnych, natomiast serwis – środków obrotowych.

Zamówienie oprogramowania bez objęcia zamówieniem płatnych poprawek i uaktualnień niezbędnych dla bieżącej konserwacji oprogramowania oraz zamówienie systemu nie obejmujące łatwych do przewidzenia zmian i rozszerzeń, a także nieuwzględnienie w określaniu zakresu zamówienia, iż po wykonaniu i wdrożeniu systemu będzie on podlegał dalszemu rozwojowi i zamianom w wyniku zmian uwarunkowań biznesowych,

prawnych czy pojawiania się nowych potrzeb. Powyższe błędy skutkowały rekomendacją, by SIWZ i umowa dla zamówień na dedykowane systemy informatyczne obejmowały wykonanie systemu wraz z możliwymi do przewidzenia zmianami i rozszerzeniami, a także z planowaną obsługą serwisową i konserwacją, chyb że planuje się zlecenie tych usług w trybie konkurencyjnym.

Ta rekomendacja jest zdecydowanie donioślejsza, albowiem prawdopodobieństwo konieczności udzielenia zamówienia z wolnej ręki na te usługi jest znacząco wyższe. Zdecydowanie należy zgodzić się ze stanowiskiem Prezesa UZP, że poprawki, aktualizacje oraz przewidywalne zmiany i rozszerzenia winny być uwzględniane od razu w opisie przedmiotu zamówienia w postępowaniu na wdrożenie systemu. Pozwoli to z jednej strony na uzyskanie warunków świadczenia tych usług w trybie konkurencyjnym, po drugie zaś na zniwelowanie różnicy między oferentami, którzy oferują stosunkowo tanie rozwiązania informatyczne, ale bardzo drogie w utrzymaniu, a wykonawcami, którzy proponują droższe rozwiązania na wejściu, ale z kolei mniej kosztowne w toku dalszej eksploatacji. Ponadto pozwoli Zamawiającemu na uniknięcie monopolizacji jednego wykonawcy, który mógłby zaproponować dowolne warunki finansowe i prawne na etapie utrzymania i rozbudowy wdrożonego systemu.

W praktyce problem dotyczy odpowiedniej kalkulacji oferty i opisu wymagań w odniesieniu do przyszłych modyfikacji, których nie się przewidzieć szczegółowo na etapie opracowywania SIWZ. Wydaje się, że w od niesieniu do tych prac możliwe jest skonstruowanie umowy o częściowo „ramowym zabarwieniu", co sprowadza się do ujęcia w ramach przedmiotu zamówienia za wykonanie, wdrożenie systemu określonej puli osobogodzin czy osobodni pracy Wykonawcy i korzystania z tego limitu w miarę potrzeb. Zwykle odbywa się to w taki sposób, że Zamawiający przedstawia Wykonawcy zakres potrzebnych modyfikacji, a Wykonawca szacuje je i ocenia ich pracochłonność, która albo zostanie zaakceptowana przez Zamawiającego, albo też Zamawiający może zrezygnować z zamówienia, jeśli strony nie porozumieją się co do warunków danej zmiany. Jest to rozwiązanie znane z umów ramowych, przy czym w przeciwieństwie do umowy ramowej, której podlega cały przedmiot danego postępowania, w tym wypadku mamy do czynienia z „ramowym" charakterem jednego ze świadczeń.

„Związanie rąk" niewielkim zamówieniem początkowym. W odniesieniu do tego błędu Prezes Urzędu zwrócił uwagę, że bardzo często zamówienie małego systemu informatycznego implikuje prowadzenie jego dalszego rozwoju przez dotychczasowego Wykonawcę (np. w wyniku przysługiwania mu praw wyłącznych do zbudowanej części systemu). Tym samym zakres zamówienia powinien być możliwie szeroki i zgodny z potrzebami określonymi na odpowiednio długim horyzoncie czasowym. Przykładów tego typu zachowań na rynku jest niestety sporo. Argumentacja Zamawiających, że takie działania służą ochronie środków publicznych przed nieuzasadnionym wydawaniem na rozbudowane systemy, podczas gdy mogą one nie spełnić oczekiwań Zamawiającego, nie wydaje się uzasadniona i to z kilku powodów. Po pierwsze, Zamawiający już na etapie przygotowywania specyfikacji istotnych warunków zamówienia winien ocenić, jakie produkty spełniają jego oczekiwania, a które nie, odbywając np. stosowne w wizyty referencyjne, testując próbki oferowanych systemów itp., a następnie odpowiednio sformułować wymagania SIWZ. Po drugie, nie jest przekonywującym argumentem zaczynanie realizacji systemu od małego wdrożenia, a następnie jego rozszerzanie w trybie niekonkurencyjnym. Takie rozwiązanie z pewnością nie będzie korzystne dla finansów publicznych i uzależni Zamawiającego od danego Wykonawcy. Sytuację tę można rozwiązać na dwa sposoby: pierwsza możliwość to zrealizowanie małego systemu, ale w sposób zapewniający Zamawiającemu prawo do rozbudowy tego systemu w trybie konkurencyjnym (np. poprzez nabycie autorskich praw majątkowych albo uzyskanie licencji na modyfikację pierwotnego systemu).

Drugie rozwiązania wydaje się konstrukcyjnie poprawniejsze: ogłoszenie przetargu na docelowe wdrożenie całego systemu, przy czym w ramach umowy przewidziane jest wdrożenie pilotowe na ograniczonym obszarze i być może z ograniczoną funkcjonalnością. Jednocześnie umowa winna przewidywać możliwość odstąpienie przez Zamawiającego od umowy po wykonaniu pilota, gdyby okazało się, że jego wyniki okażą się niesatysfakcjonujące.

Należy zauważyć, że mechanizm udzielania małego zamówienia (czasem nawet poniżej progu 14000 euro), a następnie jego rozbudowy może zostać zakwestionowany z punktu widzenia zgodności z art. 32 ust. 2 pzp, zgodnie z którym Zamawiający nie może w celu uniknięcia stosowania przepisów ustawy dzielić zamówienia na części lub zaniżać jego wartości. Wydaje się, że dotychczas ten mechanizm prawny kwestionowania prawidłowości postępowania Zamawiających nie był dostatecznie szeroko stosowany. A skutki jego zastosowania mogą okazać się bardzo doniosłe dla Zamawiającego, z unieważnieniem umowy albo jej nieważnością z mocy prawa włącznie.

Rekomendacja 4: formułowanie wymagań jakościowych, pomiar jakości i stosowanie mechanizmów zapewniania jakości w toku realizacji zamówienia

Przedmiotowa rekomendacja zawiera generalnie wskazówki dotyczące zasad określania wymagań w odniesieniu do jakości systemów informatycznych i ich weryfikowania w ramach procedur umownych. Prezes Urzędu zwraca przy tym uwagę, że niska jakość wykonanego systemu informatycznego przejawiająca się na przykład jego wysoką awaryjnością, nadmiernie skomplikowaną strukturą, niekompletną i nieczytelną dokumentacją prowadzi do uzależnienia Zamawiającego od Wykonawcy i wymusza prowadzenie rozwoju systemu informatycznego przez dotychczasowego Wykonawcę. Można więc powiedzieć, że niestaranność Wykonawcy i brak troski o jakość wytwarzanego systemu tak naprawdę sprzyja umocnieniu jego pozycji jako wyłącznego wykonawcy prac rozwojowych. Z tego względu formułuje kilka wytycznych dotyczących weryfikowania odpowiedniej jakości oprogramowania, poprzez:

a) zamieszczenie w SIWZ i umowie wymagań odnośnie jakości produktów wytwarzanych w toku realizacji projektu, trybu ustalania tych wymagań;
b) stosowanie technik zapewniania jakości, takich jak: testy modułowe, testy integracyjne, testy akceptacyjne, techniki oceny ergonomii oprogramowania, przeglądy oprogramowania i dokumentacji, metody oceny architektury (np. metody ATAM), ustalanie i stosowanie standardów kodowania, ocena spójności, kompletności, precyzji i jednoznaczności dokumentacji;
c) wprowadzenie do SWIZ możliwości dopuszczenia oceny jakości systemu przez podmiot niezależny (audyt).

Przedmiotowa rekomendacja ma zdecydowanie charakter organizacyjno-projektowy i stosunkowo w mniejszym stopniu ingeruje w konstrukcje umowne. Konieczne jest jednak przewidzenie w umowie wdrożeniowej czy innej umowie dotyczącej systemu informatycznego odpowiednich mechanizmów gwarantujących Zamawiającemu skorzystanie z tych uprawnień i ich prowadzenie w życie. Zwłaszcza w przypadku skorzystania z audytora zewnętrznego za wskazane należy uznać z jednej strony opisanie procedur współpracy Wykonawcy z takim audytorem i określenie obowiązków Wykonawcy związanych z prowadzonym audytem, z drugiej zaś mechanizmów zabezpieczających Wykonawcę przed skutkami działania audytora, jeśli audyt np. blokuje prowadzenie prac, dotrzymanie terminów umownych itp.

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

Ochrona danych osobowych a zasada otwartości w prawie Unii Europejskiej

Piotr Drobek

Zasadę jawności (otwartości) życia publicznego oraz autonomię informacyjną jednostki wiążą relacje o zróżnicowanym charakterze. Niekiedy oba dobra chronione porównuje się do awersu i rewersu tej samej monety, wskazując tym samym na ich współzależność, w pewnym zakresie wzajemne ograniczanie się, ale przede wszystkim na ich rudymentarne znaczenie dla współczesnych społeczeństw demokratycznych. W prawie Unii Europejskiej zarówno prawo publicznego dostępu do dokumentów, jak i prawo do ochrony danych osobowych są traktowane jako równorzędne prawa podstawowe. W przeważającej mierze ich realizacja przebiega w sposób harmonijny. Mogą jednak występować między nimi napięcia, rodzące również konflikty, których rozwiązanie – jak pokazuje praktyka - czasami napotyka poważne trudności. Rodzi się więc pytanie o sposób rozstrzygania możliwych sporów na styku obu praw, na które - w świetle orzecznictwa i prawa Unii Europejskiej - spróbuję skrótowo odpowiedzieć w niniejszym opracowaniu.

Gwarancje ochrony prywatności, w tym w zakresie autonomii informacyjnej jednostki, znajdziemy przede wszystkim w art. 8 europejskiej Konwencji praw człowieka i podstawowych wolności. Na gruncie prawa UE będą to: art. 7 Karty Praw Podstawowych Unii Europejskiej, który zapewnia poszanowanie życia prywatnego i rodzinnego oraz art. 8, statuujący autonomiczne prawo do ochrony danych osobowych. Regulacje dotyczące ochrony danych osobowych obecnie mają także generalną podstawę prawną w art. 16 Traktatu o Funkcjonowaniu Unii Europejskiej. Z drugiej strony Traktat o Unii Europejskiej w swym art. 1 wprost deklaruje podejmowanie decyzji z możliwie najwyższym poszanowaniem zasady otwartości i jak najbliżej obywateli. Zasada otwartości została również potwierdzona w art. 15 TFUE. Ponadto prawo do dobrej administracji oraz prawo dostępu do dokumentów statuują odpowiednio art. 41 i 42 Karty. Powołane akty prawne, a w szczególności Karta, nie przewidują szczególnych mechanizmów zapewniających rozwiązanie potencjalnych konfliktów pomiędzy prawem ochrony danych a publicznym dostępem do dokumentów. Jednakże w takiej sytuacji zastosowanie znajdą ogólne zasady przewidziane w art. 52 ust. 1 Karty, zgodnie z którym wszelkie ograniczenia w korzystaniu z praw i wolności w niej uznanych muszą być przewidziane ustawą i szanować istotę tych praw i wolności. Z zastrzeżeniem zasady proporcjonalności ograniczenia mogą być wprowadzone wyłącznie wtedy, gdy są konieczne i rzeczywiście odpowiadają celom interesu ogólnego uznawanym przez Unię lub potrzebom ochrony praw i wolności innych osób.

Oba prawa podstawowe znalazły swoje rozwinięcie w aktach prawa wtórnego, adresowanych do instytucji i organów UE. W odniesieniu do ochrony danych osobowych instytucje te początkowo odpowiednio stosowały

przepisy ogólnej dyrektywy 95/46/WE z dnia 23 października 1995 r. o ochronie osób w związku z przetwarzaniem danych osobowych oraz o swobodnym przepływie tych danych, która uszczegóławiając i rozwijając Konwencję 108 Rady Europy o ochronie danych osobowych, określiła podstawowe standardy ochrony danych osobowych w Europie i zarazem stała się punktem odniesienia dla innych regulacji z zakresu ochrony danych osobowych. Obecnie problematyka ochrony danych w instytucjach UE została uregulowana rozporządzeniem 45/2001 z dnia 18 grudnia 2000 r. o ochronie osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje i organy wspólnotowe i o swobodnym przepływie takich danych. Natomiast w odniesieniu do publicznego dostępu do dokumentów zastosowanie znajdą przepisy rozporządzenia 1049/2001 z dnia 30 maja 2001 r. w sprawie publicznego dostępu do dokumentów Parlamentu Europejskiego, Rady i Komisji. Wspomniane rozporządzenia, mające odrębne cele i przedmiot regulacji, w zasadzie nie zawierają szczególnych reguł kolizyjnych umożliwiających rozwiązywanie potencjalnych konfliktów zachodzących pomiędzy nimi, z wyjątkiem jednego przepisu art. 4 ust. 1 b rozporządzenia 1049/2001, zgodnie z którym instytucja odmówi dostępu do dokumentu, jeśli ujawnienie go naruszyłoby ochronę prywatności i integralności osoby fizycznej, w szczególności w odniesieniu do ustawodawstwa Wspólnoty związanego z ochroną danych osobowych. Interpretacja cytowanego przepisu stała się przedmiotem długoletniej i burzliwej debaty, w którą zaangażowany został szeroki krąg podmiotów, w tym m.in. Europejski Inspektor Ochrony Danych i Europejski Trybunał Sprawiedliwości. Zaowocowała ona również propozycjami zmian legislacyjnych. Warto zauważyć, że dyskusja ta została zainicjowana w związku z wnioskiem spółki Bavarian Lager skierowanym do Komisji Europejskiej. Bavarian Lager, importer piwa niemieckiego na rynek brytyjski, którego skarga stała się podstawą do podjęcia przez Komisję Europejską procedury naruszenia prawa wspólnotowego przeciwko Wielkiej Brytanii, zażądał udostępnienia protokołu ze spotkania z przedstawicielami brytyjskiej branży piwowarskiej w październiku 1996 r., po którym Komisja umorzyła toczące się dotąd postępowanie. W odpowiedzi Komisja udostępniła protokół z wyjątkiem nazwisk pięciu osób uczestniczących w spotkaniu (dwie z nich nie wyraziły na to zgody, a z trzema pozostałymi Komisja nie była w stanie się skontaktować).

Komisja swoją odmowę przede wszystkim uzasadniała interpretacją cytowanego przepisu, zgodnie z którą w stosunku do wniosku o dostęp do dokumentu zawierającego dane osobowe należy zastosować przepisy rozporządzenia 45/2001, a w szczególności jego art. 8. Przepis ten zawiera dodatkowe warunki (oprócz m. in. konieczności wykazania jednej z przesłanek legalności określonych w art. 5 tego rozporządzenia), umożliwiające przekazanie danych osobowych odbiorcom innym niż instytucje i organy wspólnotowe. W szczególności dane osobowe mogą być przekazywane jedynie odbiorcom podlegającym prawu krajowemu przyjętemu dla wykonania dyrektywy 95/46/WE, jeżeli odbiorca wykaże konieczność przekazania danych i nie ma powodu zakładać, że uprawniony interes podmiotu danych może być naruszony (art. 8 lit. b). W ocenie Komisji wnioskodawca nie wykazał takiej konieczności. Odmienną interpretację przyjął Sąd Pierwszej Instancji w swoim orzeczeniu z 8 listopada 2007 r. w sprawie Bavarian Lager v. Komisja, T-194/04, który stwierdzając naruszenie prawa przez Komisję, uznał, że wyjątek określony w art. 4 ust 1 lit b rozporządzenia 1049/2001 dotyczy tylko takiego ujawnienia danych osobowych, które może naruszać prawo do poszanowania prywatności lub integralności osoby fizycznej. Natomiast nie wymaga zastosowania przepisów rozporządzenia 45/2001, w tym m.in. konieczności wykazania konieczności

uzyskania danych zgodnie z jego art. 8 lit. b. Sąd do kryteriów oceny ingerencji w sferę prywatności wypracowanych na gruncie art. 8 europejskiej Konwencji praw człowieka i podstawowych wolności podkreślił, że „sam fakt ujawnienia uczestnictwa osoby fizycznej, w ramach pełnienia przez nią obowiązków zawodowych i jako przedstawiciela podmiotu zbiorowego, w spotkaniu z instytucją wspólnotową, przy czym nie można ustalić treści wyrażonej przez tę osobę przy tej okazji opinii osobistej, nie może zostać uznany za ingerencję w jej prywatność".

W związku z odwołaniem się Komisji od tego orzeczenia sprawa została ostatecznie rozstrzygnięta przez Trybunał Sprawiedliwości w wyroku z dnia 29 czerwca 2010 r., sprawa C-28/08 P. Trybunał, analizując okoliczności sprawy, podkreślił, że imiona i nazwiska zalicza się do danych osobowych w rozumieniu rozporządzenia 45/2001, a udostępnienie dokumentu zawierającego takie dane należy traktować jako operację przetwarzania danych osobowych. Dokonując zaś wykładni w art. 4 ust. 1 lit b rozporządzenia 1049/2001, Trybunał podkreślił, że przepis ten nie może być ograniczany jedynie do oceny naruszenia prywatności w świetle EKPC, lecz wymaga, by naruszenie prywatności i integralności osoby fizycznej było oceniane w świetle zgodności z prawodawstwem UE w zakresie ochrony danych osobowych, w tym przede wszystkim rozporządzenia 45/2001. Nie można więc rozdzielić zakresu zastosowania tego przepisu na dwie kategorie spraw: ocenianych na gruncie art. 8 EKPC i na gruncie rozporządzenia 45/2001. W konsekwencji do wniosku złożonego w trybie publicznego dostępu do dokumentów określonego w rozporządzeniu nr 1049/2001, który ma na celu uzyskanie dostępu do danych osobowych, w pełni znajdzie zastosowanie rozporządzenie 45/2001. W związku z powyższym Trybunał stwierdził, że Komisja wystarczająco zastosowała się do zasady otwartości i właściwie zażądała od Bavarian Lager wykazania konieczności przekazania danych osób, które nie udzieliły na to wyraźnej zgody.

Trybunał podkreślił również, że brak takiego uzasadnienia spowodował, iż Komisja nie miała możliwości wyważenia różnych interesów zainteresowanych stron. Notabene Trybunał także nie podjął się dokonania takiej oceny.

W dniu 24 marca 2011 r. EIOD, który w trakcie toczących się postępowań sądowych wspierał żądanie Bavarian Lager, wydał dokument poświecony zasadom publicznego dostępu do dokumentów zawierających dane osobowe po orzeczeniu Trybunału, w którym podkreślił konieczność zmian legislacyjnych w tym zakresie oraz zaproponował instytucjom przyjęcie proaktywnego podejścia, mającego na celu dokonanie właściwego balansu pomiędzy wchodzącymi tutaj w grę prawami podstawowymi w świetle zapadłego orzeczenia Trybunału. Proaktywne podejście miałoby polegać m.in. na wyważeniu wchodzących w grę interesów zanim zostanie złożony wniosek o dostęp do dokumentu i w efekcie takiego wyważenia upublicznienie go z własnej inicjatywy w trybie art. 12 rozporządzenia 1049/2001. W szczególności takiego wyważenia dóbr mógłby dokonać prawodawca, nakładając na instytucje obowiązek ujawnienia określonych dokumentów zgodnie z zasadą otwartości. Jednakże jak pokazuje wyrok Trybunału Sprawiedliwości z dnia 9 listopada 2010 r. w połączonych sprawach C-92/09 i C-93/09, dotyczący ujawniania informacji o beneficjentach pomocy z Europejskiego Funduszu Rolniczego Gwarancji i Europejskiego Funduszu Rolnego na Rzecz Rozwoju Obszarów Wiejskich, takie przepisy muszą spełniać zasadę proporcjonalności określonej w art. 52 Karty, a „ograniczenia ochrony danych osobowych powinny ograniczać się do tego, co absolutnie konieczne" i wykorzystywać „środki, które słabiej ingerują w to prawo podstawowe osób fizycznych,

a jednocześnie w skuteczny sposób przyczyniają się do realizacji celów rozpatrywanego uregulowania".

W ocenie EIOD nawet w razie braku odpowiedniego aktu legislacyjnego możliwe jest publikowanie określonych danych osobowych na podstawie wewnętrznych regulacji przyjmowanych przez instytucje, które powinny uwzględniać wyważenie wchodzących w grę interesów oraz spełniać wymogi rozporządzenia 45/2001, w odniesieniu do właściwej podstawy prawnej, spełnienia obowiązku informacyjnego oraz umożliwienia złożenia sprzeciwu.

Podsumowując, należy wskazać, że w świetle powołanego orzecznictwa dane osobowe zawarte w dokumentach publicznych nie tracą swojego charakteru, a prawo dostępu do dokumentów nie ma automatycznej przewagi nad ochroną danych osobowych i w razie konfliktu niezbędne jest dokonanie wyważenia wchodzących w grę interesów zgodnie z zasadą proporcjonalności i legalności.

Piotr Drobek - Zastępca Dyrektora Departamentu Edukacji Społecznej i Współpracy Międzynarodowej w Biurze Generalnego Inspektora Ochrony Danych Osobowych.

Polecamy

SEMINARIUM
„MODERNIZACJA I ROZBUDOWA INFRASTRUKTURY IT W FIRMIE, INSTYTUCJI I URZĘDZIE"
19 lipca 2011 r., Warszawa

Seminarium jest kierowane do szerokiej grupy odbiorców - do tych użytkowników, którzy uważają, że infrastruktura IT jest dla nich niewystarczająca - za słabe komputery, nie najnowsze oprogramowanie i do tego za małe serwery. Taka infrastruktura IT zamiast pomagać w pracy tylko ją spowalnia.
Podczas seminarium dowiedzą się Państwo, w jaki sposób można wykonać manewr przeniesienia danych, bez strat, na nowy, lepszy sprzęt i do tego nie popaść w problemy finansowe.
Zapraszamy do udziału administrację publiczną oraz przedsiębiorców.

W PROGRAMIE:
- Audyt informatyczny jako wstęp do programu modernizacji lub rozbudowy infrastruktury informatycznej. Zakres SAMowskiego audytu legalności oprogramowania. Czynniki sprzyjające złemu zarządzaniu oprogramowaniem.
- ITIL - dobre praktyki w zakresie zarządzania infrastrukturą informatyczną i jej dopasowaniem do zmieniających się potrzeb.
- Jak aktualizować i optymalizować używane w firmie oprogramowanie IT?
- Strategia zapewnienia ciągłości działania systemów informatycznych w firmach.
- Konsolidacja infrastruktury serwerowej i sieciowej - zapewnienie szybkiego dostępu do scentralizowanych aplikacji.

Więcej: www.cpi.com.pl

cpi
centrum promocji informatyki

Dobre praktyki w zarządzaniu projektami

Ewa Szczepańska

Bardzo wiele mówi się o zarządzaniu projektami, cóż to tak naprawdę oznacza? Co jest potrzebne, aby osiągnąć zamierzony cel? Czy rozwiązaniem jest zastosowanie właściwej metodyki? Czy od niej zależy sukces projektu, czy może od kierownika projektu? W poniższym artykule zostaną przedstawione najważniejsze zagadnienia, które mają znaczenie przy prowadzeniu projektu, rodzaje metodyk oraz dokumentów stosowanych podczas prowadzenia projektu.

W zależności od przedsięwzięcia, instytucji, która zajmuje się zagadnieniem, projekt może być prowadzony przy zastosowaniu jednej z kilku metodyk. Opisanie dobrych praktyk w metodyce PRINCE2 oraz PMBoK pozwala na odnalezienie wytycznych najdogodniejszych dla danej organizacji, które w konsekwencji pozwalają na prawidłowe przeprowadzenie projektu. Coraz więcej instytucji administracji publicznej stosuje metodykę PRINCE2, gdzie opisane są wskazówki dla kierownika projektu oraz dla komitetu sterującego i sponsora. Podstawowym elementem procesu zastosowania metodyki jest wyjaśnienie i usystematyzowanie pojęć związanych z zarządzaniem projektem takich, jak: projekt, zarządzanie projektem, cykl życia projektu, produkt, ryzyko, zmiana, tolerancja, pryncypia, procesy, tematy itp. Postępując zgodnie z dobrymi praktykami opisanymi w metodyce, możliwe staje się przejście przez wszystkie fazy, etapy projektu w taki sposób, aby osiągnąć zamierzony cel.

Zarządzanie projektem rozumiane jest jako „planowanie, delegowanie, monitorowanie i kontrolowanie wszystkich aspektów projektu oraz motywowanie zaangażowanych osób, aby osiągnąć oczekiwane cele projektu w granicach docelowych wskaźników wykonania, określonych dla czasu, kosztów, jakości, zakresu, korzyści i ryzyka”[1]. Natomiast projekt to „tymczasowa organizacja powołana w celu dostarczenia jednego lub więcej produktów biznesowych według uzgodnionego uzasadnienia biznesowego”[2]. Cykl życia projektu to „określenie okresu od rozpoczęcia projektu aż do przekazania ukończonego produktu tym, którzy będą go eksploatować”[3].

Wśród najczęściej stosowanych metodyk wyróżnia się: PMBoK i PRINCE2. Project Management Body of Knowledge (PMBoK) to standard utworzony przez PMI (Project

1 *PRINCE2. Skuteczne zarządzanie projektami*, wydanie 2005 TSO, str. 348
2 *PRINCE2. Skuteczne zarządzanie projektami*, wydanie 2005 TSO, str. 341
3 *PRINCE2. Skuteczne zarządzanie projektami*,

Procesy	Obszary wiedzy
Inicjowanie	Zarządzanie integralnością
Planowanie	Zarządzanie zakresem
Monitorowanie i kontrola	Zarządzanie czasem
Realizacja	Zarządzanie kosztami
Zamknięcie	Zarządzanie zasobami ludzkimi
	Zarządzanie jakością
	Zarządzanie ryzykiem
	Zarządzanie komunikacją
	Zarządzanie zaopatrzeniem

Tabela 1. Procesy oraz obszary wiedzy wg PMBoK.
Źródło: Opracowanie własne na podstawie „PMBoK", 2008.

Management Institute) opisujący dobre praktyki dla kierownika projektu z zakresu zarządzania projektem w całym cyklu jego życia. W PMBoK wyróżnia się dziewięć obszarów wiedzy i pięć grup procesów.

W skład głównych procesów wchodzą: procesy inicjowania, planowania, monitorowania i kontroli, procesy wykonawcze oraz procesy zamknięcia. Każdy proces zdefiniowany jest przez wejście i wyjście. Obszary wiedzy obejmują zagadnienia związane z zarządzaniem integralności, zakresu, czasu, kosztów, zasobów ludzkich, jakości, ryzyka, komunikacji oraz zaopatrzenia.

Druga z metodyk zajmująca się zarządzaniem projektami to PRINCE2 (**Pr**ojects **In** a **C**ontrolled **E**nvironment - projekty w środowiskach sterowalnych). Właścicielem metodyki jest OGC (Office of Government Commerce – agenda Ministerstwa Skarbu w Wielkiej Brytanii). Metodyka ta składa się z pryncypiów, czyli podstawowych zasad, procesów określających kroki, jakie należy wykonać w projekcie oraz tematów, które są grupą istotnych aspektów zarządzania i powinny znajdować się w centrum uwagi zarządzających projektem.

Poniższa tabela przedstawia wykaz pryncypiów, procesów oraz tematów, które wyróżnia się w metodyce PRINCE2.

Pryncypia	Procesy	Tematy
Ciągła zasadność biznesowa	Przygotowanie projektu	Uzasadnienie biznesowe
Korzystanie z doświadczeń	Inicjowanie projektu	Organizacja
Zdefiniowane role i obowiązki	Sterowanie etapem	Jakość
Zarządzanie etapowe	Zarządzanie końcem etapu	Plany
Zarządzanie z wykorzystaniem tolerancji	Zarządzanie dostarczeniem produktów	Ryzyko
Koncentracja na produktach	Zamykanie projektu	Zmiana
Dostosowanie do warunków projektu	Zarządzanie strategiczne projektem	Postępy

Tabela 2. Pryncypia, procesy i tematy zgodnie z PRINCE2.
Źródło: Opracowanie własne na podstawie „Skuteczne zarządzanie projektami PRINCE2", 2009.

W administracji państwowej najczęściej stosowaną metodyką jest PRINCE2, co można między innymi zaobserwować w projektach prowadzonych przez Ministerstwo Finansów, Ministerstwo Zdrowia, Ministerstwo Spraw Wewnętrznych i Administracji oraz podległych im jednostkach.

Jakie korzyści daje zastosowanie metodyki? Jakie wskazówki i zalecenia można wyciągnąć z wyżej wspomnianej metodyki?

W podręczniku Office of Government Commerce dotyczącym metodyki PRINCE2 zebrane zostały doświadczenia wielu kierowników projektów, sponsorów, zespołów projektowych, szkoleniowców, konsultantów oraz innych osób, które były zaangażowane w prowadzenie projektów. Na tej podstawie opracowano wskazówki dla osób, które rozpoczynają swoją przygodę z projektem. Stosowanie wskazanych dobrych praktyk ułatwia pracę, pozwala na planowanie, delegowanie, monitorowanie, kontrolowanie prac.

Jednym z najistotniejszych elementów skutecznego przeprowadzenia projektu jest przeszkolenie kadry zajmującej się zadaniem, czyli od członków komitetu sterującego zaczynając, a na członkach zespołu projektowego kończąc. Zwiększa to szanse na zakończenie projektu sukcesem. Jeżeli zespół projektowy posiada wiedzę w zakresie zarządzania projektem zarówno teoretyczną, jak i praktyczną, umożliwia to prawidłowe przeprowadzenie projektu i uczy spojrzenia na cały proces, przez jaki musi przejść projekt. Zdefiniowany zostaje cykl życia projektu, określone produkty, które są mierzalne, jak również opisane zostają działania, jakie powinny być wykonane, aby zrealizować projekt. Należy jednak pamiętać, że kierownik projektu ma do dyspozycji określoną liczbę zasobów, która tworzy strukturę projektową. Dzięki jasno określonym zadaniom i obowiązkom każda z osób w zespole projektowym poczuwa się do zakresu odpowiedzialności i dba o to, aby wszystko przebiegało zgodnie z planem.

Co dają dobre praktyki? Jakie są możliwe korzyści z zastosowania wybranej metodyki? Przede wszystkim wyszkolona i doświadczona kadra posługuje się jednolitym nazewnictwem, które pozwala na sprawne porozumiewanie się zarówno w zespole projektowym, jak i z wykonawcami. Możliwe staje się wprowadzenie uporządkowanych zasad i procedur podczas całego cyklu życia projektu. Poprzez zastosowanie metodyki PRINCE2 jasno określone są poszczególne role i odpowiedzialności w projekcie. Natomiast podejście produktowe opisuje, co ma zostać wytworzone, w jaki sposób odebrane, w jakich terminach i przez kogo. Każdy z elementów tematu PRINCE2 daje możliwości dobrego poprowadzenia projektu oraz wskazówki tak, aby nie zapomnieć o żadnym ważnym elemencie w projekcie.

Poprzez jasne i przejrzyste zasady użytkownicy metodyki PRINCE2 mają szanse i możliwości, aby sprawnie zarządzać projektem, identyfikować zagrożenia, wykorzystywać okazje i terminowo, zgodnie z harmonogramem wytwarzać produkty w poszczególnych etapach projektu. Klarowne określenie reguł i zestawu dobrych praktyk dla całej organizacji, począwszy od analizy kontekstu, zaangażowania interesariuszy przez cele, jasne zasady raportowania, określenie ról i odpowiedzialności oraz opracowanie wskaźników wczesnego ostrzegania, pozwalają na czerpanie korzyści w całym cyklu projektu. Dzięki spisaniu wszystkich istotnych

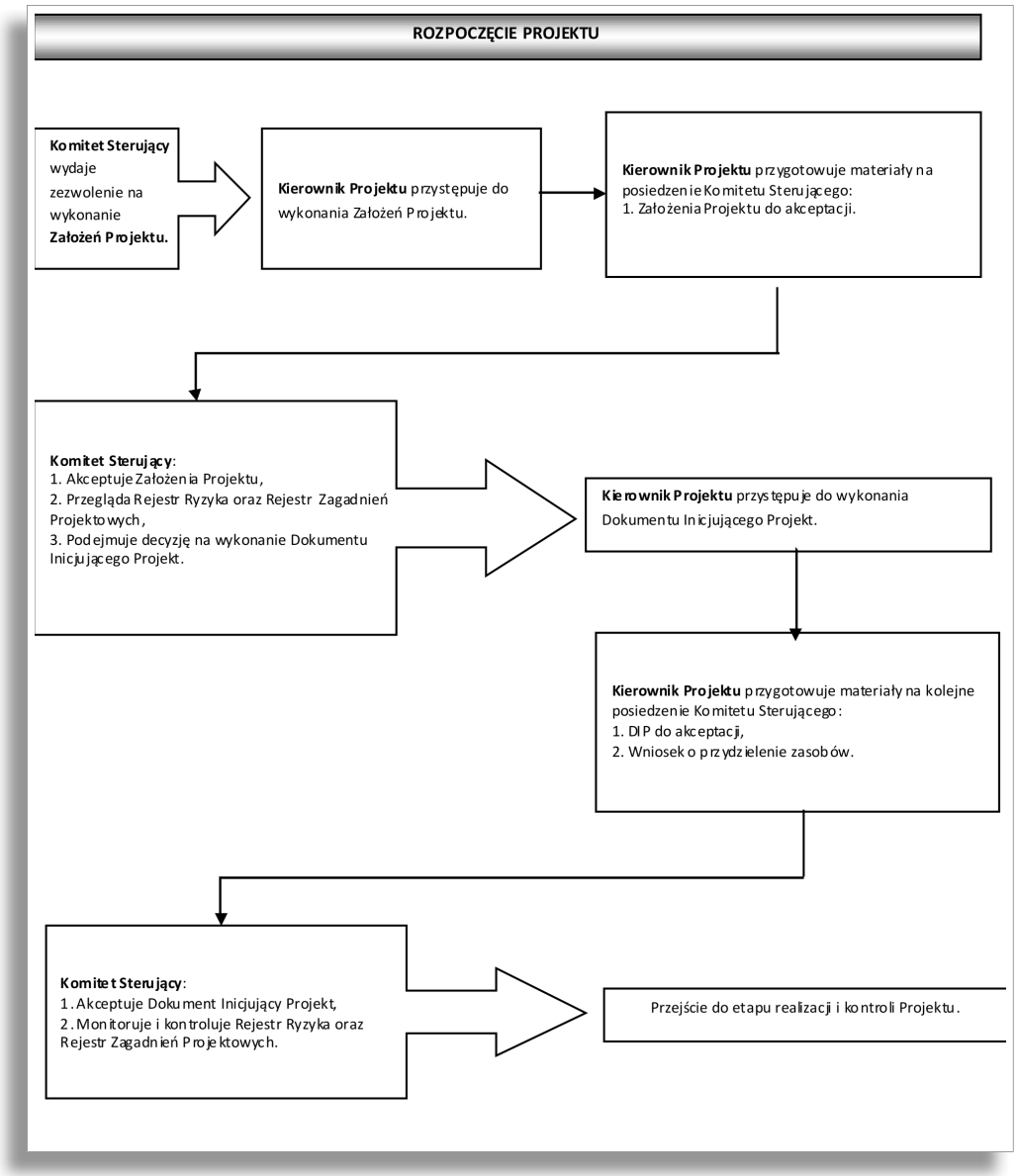
elementów w określonych szablonach dokumentów wiadome jest, gdzie należy szukać informacji oraz w jaki sposób należy postępować w określonych przypadkach. Dlatego ważne jest, aby uczestnicy biorący udział w projekcie mieli świadomość, jakie dokumenty są wytwarzane w całym cyklu życia projektu oraz gdzie należy ich szukać.

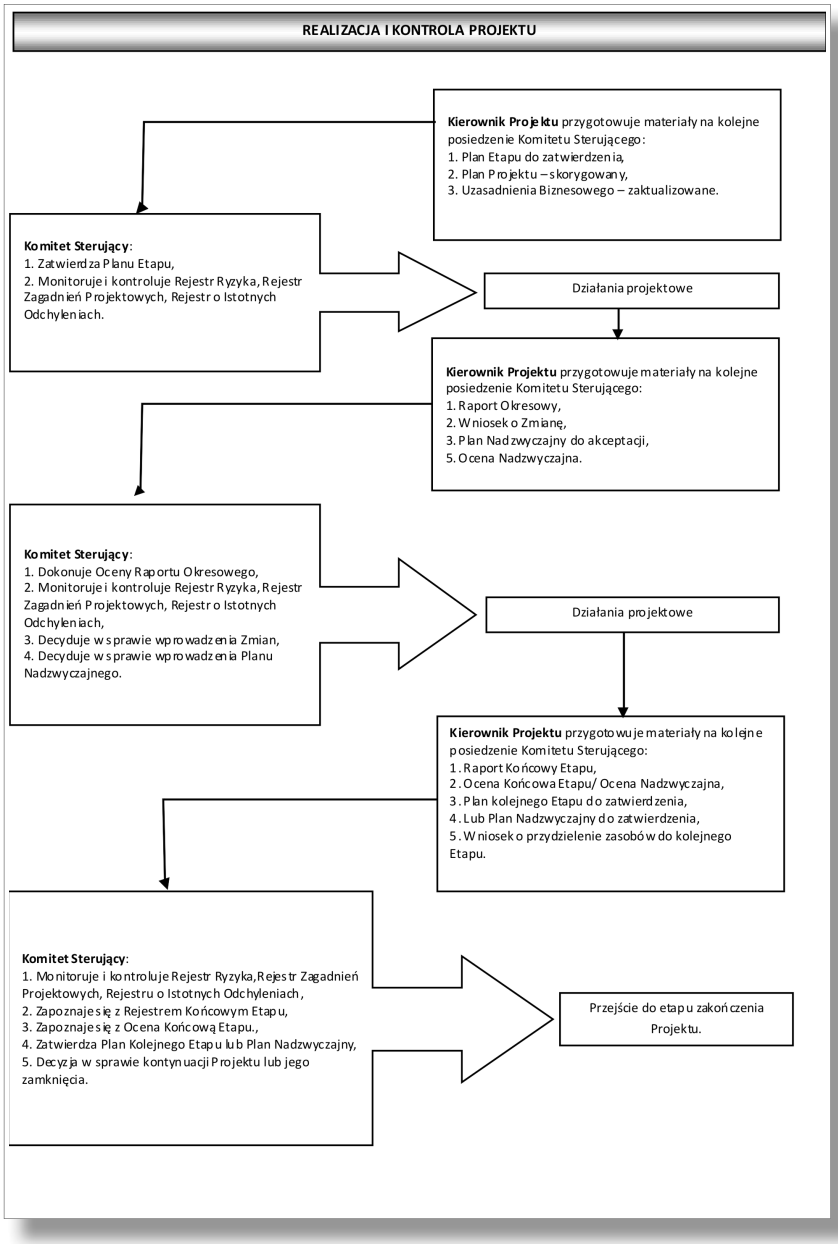
Jedną z popularnych opinii na temat metodyki PRINCE2 jest określenie jej jako zbędnej biurokracji. Każdy ma prawo do własnej opinii, jednak jak spojrzy się na to zagadnienie z szerszej perspektywy, to wprowadzenie w życie dobrych praktyk przynosi korzyści dla projektów oraz buduje bazę wiedzy, która w przyszłości będzie korzystna dla kolejnych prowadzonych przedsięwzięć, co w konsekwencji daje korzyści organizacji. Należy nauczyć się szerszego patrzenia na daną sytuację w kontekście całej organizacji, natomiast nie jest wskazane zawężanie pola widzenia poprzez postrzeganie procesów tylko i wyłącznie na jednym projekcie. To właśnie dzięki budowaniu bazy wiedzy i doświadczeniom możliwe staje się unikanie problemów i oszczędzanie czasu i pieniędzy oraz stosowanie sprawdzonych wzorów dokumentów.

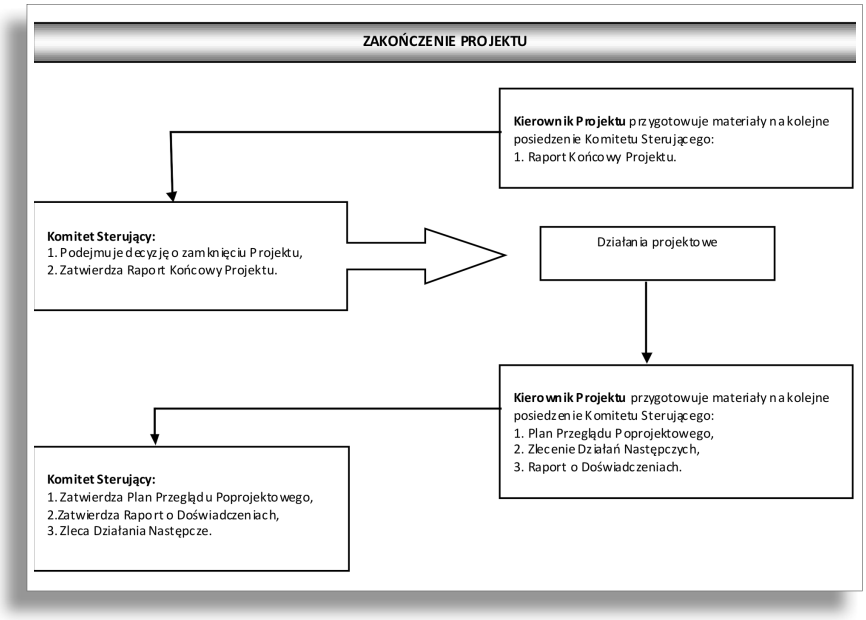
W tym momencie nasuwa się pytanie: jakie dokumenty są najważniejsze podczas prowadzenia projektu? Które raporty, plany powinien wytwarzać kierownik projektu, a z jakimi powinien zapoznawać się komitet sterujący? Wśród wytworzonej dokumentacji w projekcie mogą znaleźć się następujące raporty: z punktów kontrolnych, okresowe, o istotnych odchyleniach, doświadczeniach oraz raport końcowy projektu, raport końcowy etapu. Wśród dokumentacji dotyczącej planów zalicza się: plan zarządzania konfiguracją, przeglądu poprojektowego, plan projektu, nadzwyczajny, komunikacji, plan jakości projektu, plan etapu. W ostatniej grupie należy wymienić: rejestr jakości, rejestr zagadnień, opis produktu, listę kontrolną produktów, grupę zadań, formułę realizacji projektu, dziennik projektu, dokument inicjujący projekt, uzasadnienie biznesowe, wniosek o wprowadzenie zmiany, zlecenie działań następczych, założenia projektu, zapis obiektu konfiguracji oraz zlecenie przygotowania projektu. Wydawać by się mogło, że liczba wyżej wymienionych dokumentów jest duża, jednakże zostają one wytworzone w całym cyklu życia projektu, a należy pamiętać, że projekty często trwają od pół roku do trzech lat, a nawet dłużej. Nad całością czuwa kierownik projektu, który pilnuje, koordynuje i przekazuje stosowne informacje na temat projektu zainteresowanym osobom, czyli komitetowi sterującemu. Powstaje pytanie, w jakiej formie i jakie informacje należy przekazać osobom odpowiedzialnym za nadzór projektu, czyli przewodniczącemu komitetu sterującego, głównemu użytkownikowi i dostawcy?

Poniższe zestawienie przedstawia propozycję przekazywania dokumentów, raportów, planów przez kierownika projektu komitetowi sterującemu w trzech podstawowych fazach projektu, czyli rozpoczęciu, realizacji i kontroli oraz zakończeniu. Należy pamiętać, iż w fazie realizacji i kontroli proces informacji i obiegu dokumentów projektowych może być powtarzalny ze względu na liczbę etapów w projekcie.

Sekwencyjność przepływu informacji, dokumentów pomiędzy kierownikiem projektu a komitetem sterującym w trzech głównych etapach projektu.




REALIZACJA I KONTROLA PROJEKTU
Kierownik Projektu przygotowuje materiały na kolejne posiedzenie Komitetu Sterującego:
1. Plan Etapu do zatwierdzenia,
2. Plan Projektu – skorygowany,
3. Uzasadnienia Biznesowego – zaktualizowane.
Komitet Sterujący:
1. Zatwierdza Planu Etapu,
2. Monitoruje i kontroluje Rejestr Ryzyka, Rejestr Zagadnień Projektowych, Rejestr o Istotnych Odchyleniach.
Działania projektowe
Kierownik Projektu przygotowuje materiały na kolejne posiedzenie Komitetu Sterującego:
1. Raport Okresowy,
2. Wniosek o Zmianę,
3. Plan Nadzwyczajny do akceptacji,
5. Ocena Nadzwyczajna.
Komitet Sterujący:
1. Dokonuje Oceny Raportu Okresowego,
2. Monitoruje i kontroluje Rejestr Ryzyka, Rejestr Zagadnień Projektowych, Rejestr o Istotnych Odchyleniach,
3. Decyduje w sprawie wprowadzenia Zmian,
4. Decyduje w sprawie wprowadzenia Planu Nadzwyczajnego.
Działania projektowe
Kierownik Projektu przygotowuje materiały na kolejne posiedzenie Komitetu Sterującego:
1. Raport Końcowy Etapu,
2. Ocena Końcowa Etapu/ Ocena Nadzwyczajna,
3. Plan kolejnego Etapu do zatwierdzenia,
4. Lub Plan Nadzwyczajny do zatwierdzenia,
5. Wniosek o przydzielenie zasobów do kolejnego Etapu.
Komitet Sterujący:
1. Monitoruje i kontroluje Rejestr Ryzyka, Rejestr Zagadnień Projektowych, Rejestru o Istotnych Odchyleniach,
2. Zapoznaje się z Rejestrem Końcowym Etapu,
3. Zapoznaje się z Ocena Końcową Etapu.,
4. Zatwierdza Plan Kolejnego Etapu lub Plan Nadzwyczajny,
5. Decyzja w sprawie kontynuacji Projektu lub jego zamknięcia.
Przejście do etapu zakończenia Projektu.



Źródło: Opracowanie własne.

Decyzja o zastosowaniu poszczególnych dokumentów w projekcie uzależniona jest przede wszystkim od wielkości projektu. Nie jest zasadne, aby w małym projekcie stosować wszystkie dokumenty, które proponuje podręcznik OGC „PRINCE2 - Skuteczne zarządzanie projektami", ponieważ w takim przypadku można by mówić rzeczywiście o biurokracji i stracie czasu na zbędne produkowanie dokumentów. Dlatego też każda organizacja dokonuje wyboru, jakie elementy z metodyki PRINCE2 będzie stosowała w zależności od swoich możliwości i potrzeb.

W powyższym artykule skupiono się przede wszystkim na przedstawieniu głównych założeń metodyki PRINCE2 oraz możliwościach wykorzystania proponowanej dokumentacji.

W każdym z elementów metodyki, czy to będzie mowa o pryncypiach, tematach czy procesach, zawsze można odnaleźć wskazówki i dobre rady, aby podczas pracy unikać błędów, aby sprawnie następował przepływ informacji oraz aby w organizacji i projekcie każda osoba potrafiła identyfikować się ze swoimi zadaniami i wiedziała, jaka odpowiedzialność na niej spoczywa. Bazę wiedzy, zbiory praktyk buduje się po to, aby ułatwić i usprawnić pracę wszystkim zainteresowanym. Jeśli ktoś przed nami otworzył już drzwi, to lepiej jest przez nie przejść, niż bić głową w mur.

Bibliografia:

1. *A guide to Project Management Body of Knowledge*, 2008, PMI,
2. *PRINCE2. Skuteczne zarządzanie projektami*, wydanie 2009 TSO,
3. *PRINCE2. Skuteczne zarządzanie projektami*, wydanie 2005 TSO.

Ewa Szczepańska - od ponad 11 lat uczestniczy w budowie i wdrażaniu systemów IT dla potrzeb administracji państwowej.

Problemy w projektach informatycznych realizowanych na potrzeby administracji publicznej

Izabela Adamska

W obrocie gospodarczym coraz bardziej powszechna staje się komunikacja elektroniczna, która znacznie usprawnia przepływ informacji zarówno w organizacji, jak i w kontaktach zewnętrznych. Internet wkracza w różne sfery naszego życia, proponując nowe rozwiązania. Dziś trudno wyobrazić sobie świat bez komputerów, a dzięki nieograniczonemu dostępowi do Internetu można załatwić codzienne sprawy: sprawdzić stan konta bankowego, zapłacić bieżące rachunki, zrobić zakupy, złożyć wniosek do urzędu, zawierać umowy z kontrahentami, czy nawet zobaczyć się z bliskimi przebywającymi w innym kraju. Wszystkie te czynności są możliwe dzięki zastosowaniu systemów teleinformatycznych. Coraz powszechniejsze staje się wykorzystanie potencjału technologicznego do tworzenia produktów i usług, co zmierza do wykreowania w przyszłości nowych potrzeb lub zaspokojenia istniejących potrzeb w inny, nowy sposób.

Dynamiczny rozwój technologiczny, którego jesteśmy świadkami na przestrzeni ostatnich lat, spowodował znaczny wzrost nakładów finansowych na rozwój technologii informacyjnych. Dzięki zastosowaniu narzędzi informatycznych możliwe jest szybkie i skuteczne wykonywanie zadań z różnych dziedzin. Zanim jednak to nastąpi, konieczne jest zmierzenie się z rzeczywistością, czyli sprawne przeprowadzenie projektu[1] informatycznego. W tym celu konieczne jest spełnienie trzech warunków jednocześnie:

- uzyskania zamówionego rozwiązania w określonym czasie,
- utrzymania budżetu projektu na zaplanowanym poziomie,
- otrzymania rozwiązania spełniającego wymagania (zakres) przy zapewnieniu określonej jakości.

Spełnienie wszystkich wymienionych wyżej warunków jednocześnie jest skomplikowanym przedsięwzięciem i wymaga zaangażowania odpowiednich zasobów oraz ich właściwego rozłożenia w czasie (sprawnego zarządzania projektem). Wiedza w zakresie realizacji projektów IT wciąż się zwiększa, a metodyki i narzędzia wspomagające zarządzanie ewoluują, mimo to problemy w projektach są zjawiskiem powszechnym. Dotykają one czterech podstawowych parametrów projektu: czasu, budżetu, zakresu i jakości (trójkąt ograniczeń). Nie jest możliwe utrzymanie wszystkich parametrów w równym stopniu na wysokim poziomie. Jeśli zostanie skrócony czas przy zachowaniu zakresu projektu, to odpowiednio należy zwiększyć budżet. Jeśli tak się nie stanie, będzie to miało negatywny wpływ na jakość produktów projektu. Zmiana więcej niż dwóch parametrów powoduje naruszenie równowagi trójkąta, co oznacza niepowodzenie projektu. Można pokusić się o stwierdzenie, że zarządzanie projektem jest „ciągłą

1 Projekt to wiele problemów o różnym stopniu skomplikowania, rozłożonych w czasie.

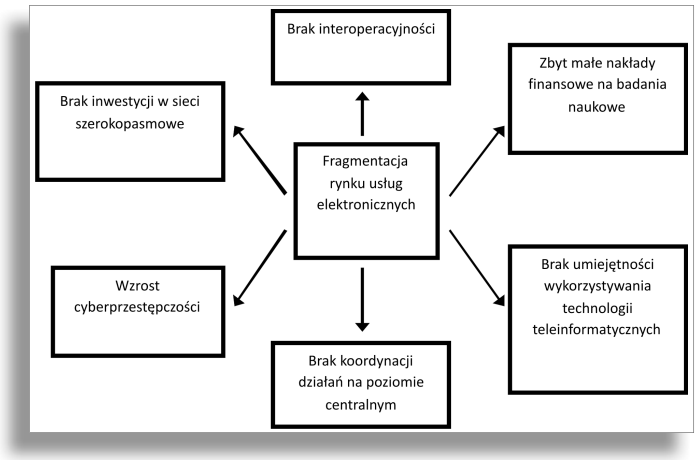
walką o zachowanie równowagi trójkąta ograniczeń". Metodyki zarządzania, wspomagając sprawną realizację projektu, tak naprawdę skupiają się na kontrolowaniu parametrów trójkąta.

Specyfika administracji publicznej

Budowa w Polsce jednolitego rynku usług administracji publicznej świadczonych drogą elektroniczną pozostaje nadal niezakończona. Brak koordynacji działań w skali kraju doprowadził do rozproszenia systemów informacyjnych jednostek administracji publicznej, budowanych w oderwaniu od innych systemów informacyjnych, bez dzielenia się wiedzą i doświadczeniem. Wynikiem takiego działania jest fragmentacja rynku usług publicznych on-line. Dodatkową barierą jest brak dostępu do sieci szerokopasmowych dla wszystkich obywateli, co jest spowodowane brakiem wystarczających inwestycji w budowę sieci szerokopasmowych. Wciąż jeszcze spora część społeczeństwa pozostaje wykluczona cyfrowo czy to z braku infrastruktury, czy też z braku umiejętności wykorzystania dostępnej technologii.

Ponadto duża grupa jednostek samorządu terytorialnego odnosi się niechętnie do przeniesienia usług publicznych do wirtualnej rzeczywistości. Jest to widoczne na przykładzie jednego ze strategicznych systemów informatycznych państwa - elektronicznej Platformy Usług Administracji Publicznej (ePUAP). W ramach działań zmierzających do integracji regionalnych systemów dziedzinowych z elektroniczną Platformą Usług Administracji Publicznej (ePUAP) został przygotowany dokument „Linia Współpracy. Założenia architektury współdziałania infrastruktur rządowej i samorządowej (centralnej i regionalnej) w procesie realizacji zadań publicznych" w celu wykreowania wizji współdziałania regionalnych systemów administracji publicznej służących dostarczaniu usług publicznych z centralną platformą ePUAP. Dokument ma umożliwić określenie zakresów projektów oraz określić zasady współpracy i odpowiedzialności administracji rządowej i samorządowej w procesie rozwoju infrastruktury informatycznej państwa zapewniający interoperacyjność, w szczególności poprzez:

- określenie głównych funkcjonalności centralnej platformy ePUAP,
- określenie zakresu współdziałania systemów (interfejsy logiczne) regionalnych i centralnej platformy ePUAP,
- określenie ram prawnych współpracy,



Rys 1.
Źródło: opracowanie własne

- podział przestrzeni funkcjonalności związanych z dostarczaniem usług publicznych pomiędzy systemy regionalne oraz centralną platformę ePUAP.

Stworzenie integratora usług publicznych było słuszną decyzją i w dłuższej perspektywie przynoszącą wymierne korzyści zarówno obywatelom, jak i administracji (szczególnie samorządowej – świadczącej usługi dla obywateli). Elektroniczna Platforma Usług Administracji Publicznej (ePUAP) nie zastępuje systemów dziedzinowych, ale wymaga współdziałania lokalnych systemów teleinformatycznych dostarczających usługi publiczne. Pozwoli to zapewnić interoperacyjność, czyli zdolność systemów teleinformatycznych do efektywnej współpracy w celu zapewnienia wzajemnego dostępu użytkowników do usług świadczonych w tych systemach. ePUAP udostępnia usługi jednostkom administracji rządowej i samorządowej (jak np. Elektroniczna Skrzynka Podawcza, Centralne Repozytorium Wzorów Dokumentów Elektronicznych) oraz zawiera katalog usług elektronicznych oferowanych przez podmioty świadczące takie usługi (np. wycinka drzew). Jednak udostępnienie usług za pośrednictwem komunikacji elektronicznej pozostaje w kompetencjach jednostek samorządu terytorialnego.

Czy projekty informatyczne realizowane przez administrację publiczną wyróżniają się czymś szczególnym? Jakie problemy występują w projektach IT administracji publicznej zarówno na etapie przygotowania, jak i realizacji?

Projekty informatyczne realizowane w jednostkach administracji publicznej w dużej mierze mają na celu upowszechnienie świadczenia usług publicznych, co prowadzi do usprawnienia elektronicznego kontaktu obywatela z administracją publiczną, a więc świadczenia usług drogą elektroniczną. Dla właściwego zrozumienia zagadnienia, należy spojrzeć na problemy realizacji projektów informacyjnych w administracji poprzez problemy wynikające ze świadczenia usług publicznych drogą elektroniczną. Oczywiście, jak w przypadku każdego rozwiązania informatycznego, jest możliwość zakupienia istniejącego systemu (tzw. „z pudełka"), dostosowania istniejącego rozwiązania do własnych potrzeb oraz zamówienia rozwiązania dedykowanego. Definiowanie wymagań należy rozpocząć od analizy istniejących procesów w organizacji, niezależnie od tego czy będzie to mała gmina, czy duże miasto.

Administracja publiczna prowadzi ciekawe i duże projekty, których realizacja wiąże się ze sporymi nakładami finansowymi. Cel projektów jest podobny – zastosowanie rozwiązania IT ma poprawić jakość życia obywateli, a więc tak samo ważne jest właściwe uzasadnienie biznesowe projektu, określenie parametrów systemu oraz właściwe oszacowanie czasu, budżetu, zakresu projektu. Nie należy zapominać o interesariuszach projektu, mając na uwadze rozbieżność interesów wszystkich zainteresowanych, a przede wszystkim użytkowników końcowych. Administracja publiczna definiuje przede wszystkim wymagania systemu informatycznego, procesy, jakie będzie on realizował oraz sformułuje wymagania dotyczące utrzymania i rozwoju systemu, a także dokona odbioru rozwiązania.

W perspektywie rozwoju usług publicznych świadczonych drogą elektroniczną problemy pojawiające się w projektach systemów informacyjnych nabrały innego znaczenia. Zważywszy na strukturę e-government, należy rozpatrywać przyczyny problemów w projektach IT w podanych niżej kategoriach. Problemy zostały sklasyfikowane i podzielone na cztery grupy. Podział barier wdrożeniowych systemów informatycznych został dokonany w IDABC[1].

2 *E-Government Factsheet – Finland – Strategy,* http://ec.europa.eu/idabc/en/document/6068/392, listopad 2004 oraz Oskar Szumski, *E-procurement. Systemy elektronicznych zamówień publicznych,* Wydawnictwo Difin, Warszawa 2007.

Grupa I	**Rozwój, implementacja oraz dostarczenie usług publicznych drogą elektroniczną**
	1. Złożone i niespójne procedury administracji publicznej. 2. Brak wspólnej strategii świadczenia usług publicznych świadczonych drogą elektroniczną na poziomie centralnym. 3. Brak ogólnie stosowanych standardów dokumentów w postaci elektronicznej. 4. Brak wymiany danych pomiędzy jednostkami administracji publicznej, a także pomiędzy komórkami w obrębie jednostek administracji publicznej – ograniczone wykorzystanie rejestrów publicznych – pomimo wejścia w życie nowelizacji ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne. 5. Brak doświadczenia we wdrażaniu systemów informatycznych. 6. Słaba koordynacja działań pomiędzy administracja rządową a samorządową – niezatwierdzony dokument „Linia Współpracy. Założenia architektury współdziałania infrastruktur rządowej i samorządowej (centralnej i regionalnej) w procesie realizacji zadań publicznych". 7. Fragmentaryczne systemy informacyjne, brak integracji. 8. Brak współdzielenia informacji zgromadzonych przez administrację publiczną. 9. Słaba dynamika rozwoju portali administracji publicznej. 10. Struktura resortowa administracji publicznej. 11. Długotrwała procedura związana ze stosowaniem prawa zamówień publicznych. 12. Skomplikowane i niespójne procedury administracyjne dotyczące świadczenia usług za pomocą komunikacji elektronicznej. 13. Niespójne regulacje prawne dotyczące elektronicznej administracji, np. obligatoryjność wykorzystywania podpisu własnoręcznego przy załatwianiu wielu spraw administracyjnych. 14. Ograniczone zasoby zaangażowane w rozwój e-administracji. 15. Informatyzacja rozumiana jako komputeryzacja.
Grupa II	**Popyt na usługi publiczne dostępne drogą elektroniczną oraz ich jakość**
	1. Brak jednolitego źródła informacji powodujący dezorientacje obywateli. 2. Niechęć do udzielania informacji publicznej mimo funkcjonowania ustawy z dnia …. o dostępie do informacji publicznej. 3. Brak odpowiedniej wiedzy o możliwości świadczenia usług publicznych przez Internet. 4. Niewystarczająca znajomość potrzeb użytkowników w zakresie e-administracji – brak zainteresowania rzeczywistymi oczekiwaniami użytkowników dotyczącymi e-usług. 5. Obawa przed wdrożeniem i wykorzystaniem nowych rozwiązań teleinformatycznych. 6. Brak spójnego podejścia do rozwoju usług administracji publicznej (duplikowanie działań). 7. Brak kryteriów oceny jakości usług administracji publicznej świadczonych drogą elektroniczną. 8. Nikłe zaangażowanie obywateli w działania administracji publicznej na wszystkich szczeblach.
Grupa III	**Dostępność, łatwość wykorzystania systemu oraz umiejętności użytkowników**
	1. Niewystarczająca wiedza użytkowników w zakresie wykorzystania narzędzi teleinformatycznych, powodująca brak przekonania obywateli o skuteczności kontaktu elektronicznego z administracją publiczną. 2. Brak powszechnego zastosowania w jednostkach administracji publicznej bezpiecznego podpisu elektronicznego, czytników kart. 3. Duplikowanie informacji, chaos informacyjny w sieci. 4. Brak integracji lub utrudniona integracja systemów informatycznych ze względu na zastosowanie różnych technologii i standardów. 5. Obawa o bezpieczeństwo danych znajdujących się w systemie teleinformatycznych. 6. Ograniczony szerokopasmowy dostęp do sieci szerokopasmowych – duża grupa społeczeństwa jest wykluczona cyfrowo. 7. Brak zaufania do bezpieczeństwa przetwarzanych danych w ramach e-usług.

	Nadawanie kierunku oraz koordynacja rozwoju systemu usług publicznych dostępnych drogą elektroniczną
Grupa IV	1. Uwarunkowania polityczne mające wpływ na kierunki rozwoju e-administracji. 2. Skomplikowana i długotrwała procedura wdrażania nowych regulacji. 3. Brak koordynacji na poziomie centralnym działań administracji publicznej w zakresie budowy i rozwoju systemów teleinformatycznych oraz w zakresie rozwoju usług administracji publicznej świadczonych drogą elektroniczną. 4. Brak uwarunkowań prawnych dotyczących standardów świadczenia usług drogą elektroniczną (31 grudnia 20010 roku wygasło rozporządzenie w sprawie minimalnych wymagań dla systemów teleinformatycznych, a Krajowe Ramy Interoperacyjności, które mają zastąpić wspomniane rozporządzenie, są obecnie na etapie konsultacji). 5. Długotrwały proces prowadzący do inicjacji projektu oraz formalizacja działań.

Tabela 1.

Warto sobie zadać pytanie, co leży u źródła problemów pojawiających się podczas realizacji projektów informatycznych w jednostkach administracji publicznej? Strategiczne projekty informatyczne realizowane na potrzeby administracji są projektami trudnymi/o dużym stopniu skomplikowania (szczególnie dotyczy to projektów związanych z e-administracją). Na swojej drodze napotykają na bariery specyficzne tylko dla sektora publicznego (tabela) oraz problemami związanymi stricte z budową, rozwojem i utrzymaniem systemów informatycznych. Przyczyny niepowodzeń projektów zostały zbadane przez The Standish Group. W raporcie zatytułowanym *Chaos*[3] publikowanym przez tę organizację można zapoznać się ze statystykami dotyczącymi projektów IT. Projekty klasyfikowane są w następujących kategoriach:

- zakończone sukcesem (32%) – czyli projekty, które zostały zrealizowane w zakładanym czasie, budżecie i pełnym zakresie (możliwe są odstępstwa od zakładanych wartości tych parametrów w zakresie ustalonych tolerancji). Oznacza to, że 1/3 realizowanych projektów dostarczana jest na czas, mieści się w budżecie i posiada wyspecyfikowane na etapie planowania funkcjonalności.
- zakończone częściową porażką (44%) – w których produkt finalny jest kompletnym i działającym produktem, lecz został przekroczony budżet, czas realizacji lub projekt został zrealizowany w mniejszym niż zakładano zakresie. Aż 44% projektów ma opóźnienie, został przekroczony budżet lub produkty projektu posiadają mniejsze funkcjonalności niż wymagane.
- zakończone porażką (anulowane) (24%) – czyli projekty, których realizacja została przerwana lub produkt finalny nie został osiągnięty w stopniu umożliwiającym jego eksploatację[4].

Wyniki raportu wskazują na to, że jedynie 1/3 wszystkich projektów zakończyła się sukcesem.

Jak rozwiązywać problemy?

Sposobem na rozwiązanie problemów, a tym samym na kontrolę procesu realizacji projektu IT, jest odpowiednie zaadoptowanie metodyki zarządzania, np. metodyki PRINCE2. Podstawowym celem metodyki jest stworzenie standardu

3 *Raport Chaos 2009* opracowany przez Standish Group.
4 *Raport Chaos 2009* opracowany przez Standish Group.
5 Metodykę zarządzania projektami można określić jako zbiór procedur oraz zasad skutecznego zarządzania projektem. Każdy etap zakończony jest odbiorem produktów cząstkowych projektu.

w organizacji, co pozwoli zapewnić uporządkowane, przemyślane i spójne prowadzenie projektów o różnym stopniu skomplikowania i różnej wielkości. Metodyka powinna być elastyczna i dostosowana do projektów o różnej skali w odniesieniu do specyfiki projektu. Skuteczne zarządzanie projektami jest wynikiem wielu czynników, między innymi osiągania założonych celów przy uwzględnieniu otoczenia zewnętrznego, doświadczenia czy też efektywnego wykorzystania zasobów. Dużą rolę odgrywa również zaangażowanie w realizację projektu – nie tylko kierownika projektu i zespołu, ale również głównych interesariuszy projektu. Nie ma prostych i przewidywalnych projektów. Należy konsekwentnie dążyć do postawionych celów, nie zapominając o elastyczności pozwalającej dopasować rozwiązanie do zmieniających się warunków, zachowując właściwe proporcje pomiędzy elementami decydującymi o powodzeniu projektu. Według badań przeprowadzonych przez organizację The Standish Group są to:

- zaangażowanie klienta – 15,9%,
- wsparcie kierownictwa – 13,9%,
- jasno określone wymagania – 13,0%,
- właściwe planowanie – 9,6%,
- realistyczne oczekiwania – 8,2%,
- mniejsze odstępy pomiędzy kamieniami milowymi – 7,7%,
- kompetencje pracowników – 7,2%,
- odpowiedzialność – 5,3%,
- jasno postawione cele i wymagania – 2,9%,
- ciężko pracujący, skupieni pracownicy – 2,4%,
- pozostałe – 13,9%.

Kryteria te wskazują, że u przyczyn niepowodzeń projektu leżą przede wszystkim błędy w zarządzaniu, a także dotyczą czynnika ludzkiego, czyli zaangażowania, kompetencji, odpowiedzialności. W projektach informatycznych często pojawiają się trudności kończące się niepowodzeniem projektu. „W niemal trzech czwartych wszystkich przedsięwzięć polegających na tworzeniu oprogramowania w dobie Internetu wystąpiło przynajmniej jedno z następujących zjawisk: kompletne niepowodzenie, przekroczenie kosztów, przekroczenie terminów albo powstanie produktu”[6] o funkcjonalnościach nieodpowiadających oczekiwaniom użytkowników. „Około 85% projektów informatycznych w sektorze publicznym uważa się za nieudane... Choć nie oznacza to, że kończą się one kompletną klapą, ale zwykle przedłuża się ich realizacja, wzrastają koszty, a rezultaty są skromniejsze niż planowano”[7]. Znacznie poważniejsze są jednak straty wynikające z niewykorzystanych szans, niezrealizowanych strategii, braku optymalizacji procesów biznesowych w organizacji, utraty wiarygodności oraz spadku wydajności członków zespołu.

Izabela Adamska - pracownik administracji publicznej.

6 *Raport Chaos 2009* opracowany przez Standish Group.
7 *Raport Chaos 2009* opracowany przez Standish Group.

Wyrok Krajowej Izby Odwoławczej z dnia 20 lipca 2010 r., sygn. akt: KIO 1408/10

Wojciech Kaliński

… Wszystkie wskazane w §2 ust. 2 złożonej przez ... gwarancji ubezpieczeniowej zapłaty wadium zdarzenia odnoszą się jedynie do jednego z podmiotów wspólnie ubiegających się o udzielenie zamówienia publicznego i wobec faktu złożenia przez podmiot określony w treści gwarancji jako oferent (uczestnik przetargu) oferty wraz z innym podmiotem na podstawie art. 23 ust. 1 ustawy pzp powodują, iż w stosunku do oferty złożonej przez wykonawców wspólnie ubiegających się o udzielenie zamówienia wadium nie zostało skutecznie wniesione. Powyższe wynika z faktu, iż wskazane w treści gwarancji ubezpieczeniowej okoliczności nie są zupełne i nie obejmują wszystkich możliwych zdarzeń, które mogą spowodować prawo żądania przez Zamawiającego zapłaty kwoty gwarancyjnej.

Przedmiotowy wyrok zapadł w niezwykle ciekawiej sprawie dotyczącej wniesienia wadium w postaci gwarancji ubezpieczeniowej wystawionej na zlecenie jednego z podmiotów w sytuacji, gdy podmiot ten złożył ofertę, występując w konsorcjum w rozumieniu art. 23 ust. 1 pzp. Z przedstawionego w wyroku stanu faktycznego wynika, że uczestnik postępowania zlecił firmie ubezpieczeniowej wystawienie gwarancji wadialnej firmie ubezpieczeniowej, występując w przetargu wspólnie z innym wykonawcą. Tymczasem treść gwarancja ubezpieczeniowej (wadialnej) została tak skonstruowana, jakby zleceniodawca uczestniczył w przetargu samodzielnie. Na tle tego stanu faktycznego powstało więc pytanie, czy gwarancja ubezpieczeniowa wystawiona na zlecenie jednego z wykonawców występujących wspólnie w rozumieniu art. 23 ust. 1 pzp, wskazująca jedynie zleceniodawcę jako uczestnika postępowania, spełnia wymagania w zakresie skutecznego wniesienia wadium na potrzeby postępowania przetargowego.

Przedstawione pytanie można również rozszerzyć na inne postacie wadium, w szczególności, choć nie wyłącznie, na gwarancję bankową oraz poręczenie. Problem ograniczonego zakresu wadium może również dotyczyć wadium pieniężnego, gdy w opisie przelewu znajdą się sformułowania ograniczające jego znaczenie tylko do jednego z konsorcjantów. Tym samym na gruncie analizowanego wyroku KIO pojawia się pytanie, jak ocenić skuteczność wadium wniesionego na rzecz jednego z wykonawców spośród wykonawców wspólnie uczestniczących w postępowaniu o udzielenie zamówienia publicznego?

W pierwszej kolejności należy obalić mit, powszechnie funkcjonujący w systemie zamówień publicznych, o solidarnej odpowiedzialności wykonawców, składających wspólną ofertę. Zgodnie z art. 141 pzp wykonawcy, o których mowa w art. 23 ust. 1, ponoszą solidarną odpowiedzialność za wykonanie umowy i wniesienie zabezpieczenia należytego wykonania umowy. Oznacza to, a contrario, brak solidarności w zakresie nieobjętym przedmiotowym przepisem, a zatem przed wniesieniem zabezpieczenia należytego wykonania umowy oraz przed zawarciem umowy. Zobowiązanie jest bowiem solidarne, jeżeli to wynika z ustawy lub z czynności prawnej (art. 369 k.c.). Na etapie składania ofert solidarność wykonawców występujących wspólnie nie wynika z treści oferty ani przepisów ustawy – Prawo zamówień publicznych. Ponieważ wykonawcy, składając ofertę, nie zaciągają zobowiązania dotyczącego ich wspólnego mienia, solidarność nie będzie również wynikać z treści art. 370 k.c. Oznacza to, że złożenie oferty przez wykonawców występujących wspólnie na podstawie art. 23 ust. 1 pzp skutkuje powstaniem stosunku prawnego, gdzie po stronie oferenta mamy do czynienia z sytuacją wielopodmiotowości, lecz nie opartej o konstrukcję solidarności. Konsekwencją tego stanu rzeczy jest fakt, że zamawiający może żądać wykonania przez „konsorcjum" obowiązków wykonawcy wynikających z SIWZ i ustawy tylko łącznie od wszystkich wykonawców występujących wspólnie. Konstrukcji tej sprzyja zresztą wyrażony w art. 23 ust. 2 pzp obowiązek ustanowienia pełnomocnika co najmniej do reprezentowania wykonawców w postępowaniu o udzielenie zamówienia. Tym samym czynności pełnomocnika, jak czynności zamawiającego skierowane pod adresem pełnomocnika, skutkują wobec wszystkich uczestników konsorcjum.

Powstaje zatem pytanie, jak do powyższych zasad ma się wniesienie wadium przez jednego z konsorcjantów? W tym miejscu należy zastrzec, że z faktu, iż żądania kierowane do konsorcjum winny domagać się określonego zachowania od wszystkich wykonawców, nie oznacza, iż faktycznie daną czynność musi wykonać oddzielnie każdy z nich. Wystarczy bowiem, że wymaganej czynności dokona jeden z nich, pod warunkiem że czynność ta będzie skuteczna wobec wszystkich pozostałych wykonawców działających w trybie art. 23 pzp. Innymi słowy, działać może każdy z wykonawców, o ile działanie to wywoła skutek względem pozostałych. Analogicznie należy ocenić wniesienie wadium. Może ono zostać wniesione przez każdego z wykonawców, o ile wywoła skutek względem pozostałych. W sytuacji, w której z treści dokumentu wadialnego (czy to gwarancji ubezpieczeniowej, czy bankowej, poręczenia czy nawet treści przelewu) wynika, że przedmiotowe świadczenie czy zobowiązanie zabezpiecza określone zachowania tylko jednego z wykonawców, wadium takie będzie niewystarczające. W przypadku gwarancji i poręczeń trzeba mieć bowiem na uwadze, że o zakresie odpowiedzialności ubezpieczyciela decyduje zakres jego zobowiązania. Dobrze ilustrują ten problem przepisy prawa bankowego. Zgodnie z art. 81 ust. 1 pr. bankowego gwarancją bankową jest jednostronne zobowiązanie banku-gwaranta, że po spełnieniu przez podmiot uprawniony (beneficjenta gwarancji) określonych warunków zapłaty, które mogą być stwierdzone określonymi w tym zapewnieniu dokumentami, jakie beneficjent załączy do sporządzonego we wskazanej formie żądania zapłaty, bank ten wykona świadczenie pieniężne na rzecz beneficjenta gwarancji - bezpośrednio albo za pośrednictwem innego banku. Jak słusznie zauważa J. Pisuliński (J. Pisuliński w: Bączyk Mirosław, Góral Lesław, Fojcik-Mastalska Eugenia (redakcja), Pisuliński Jerzy, Pyzioł Wojciech, *Prawo bankowe. Komentarz*, Warszawa 2007, Wydawnictwo Prawnicze LexisNexis, s. 840) w komentarzu do tego przepisu: „*Art. 81 ust. 1 można uznać za ustawową próbę definicji gwarancji. Definicja ta jednak nie jest kompletna ani*

ścisła. Dlatego na podstawie całości przepisów Prawa bankowego gwarancję bankową można określić jako zobowiązanie zaciągnięte przez bank (gwaranta) na zlecenie innej osoby (zleceniodawcy gwarancji), na mocy którego bank obowiązany jest do zapłaty pewnej sumy pieniężnej (w złotych lub walucie obcej) na żądanie osoby uprawnionej (beneficjenta gwarancji) po spełnieniu przez nią określonych przesłanek (verba legis: warunków)." oraz: „*Zobowiązanie banku wobec beneficjenta gwarancji powstaje dopiero wskutek złożenia przez bank oświadczenia o udzieleniu gwarancji. Treść oświadczenia banku powinna odpowiadać warunkom ustalonym w umowie łączącej bank ze zleceniodawcą gwarancji. W razie rozbieżności między umową zawartą ze zleceniodawcą a treścią oświadczenia banku o udzieleniu gwarancji o zakresie zobowiązania banku decyduje treść złożonego przez niego oświadczenia. Wymaga tego ochrona zaufania beneficjenta gwarancji, który na ogół nie będzie znał treści umowy łączącej gwaranta ze zleceniodawcą, tworzącej stosunek pokrycia. Bank udzielający gwarancji nie może się powoływać wobec beneficjenta na zarzuty wynikające ze stosunku pokrycia (zob. dalsze uwagi w pkt 37, a także uzasadnienie wyroku SN z 22 stycznia 2002 r., V CKN 637/2000, OSNC 2003, nr 4, poz. 49).*" Tym samym zawarte w gwarancji wadialnej sformułowania określające przesłanki utraty wadium w postaci sformułowania: „- *Oferent odmówił podpisania umowy w sprawie zamówienia publicznego na warunkach określonych w ofercie; - Oferent nie wniósł wymaganego zabezpieczenia należytego wykonania umowy; - zawarcie umowy w sprawie zamówienia publicznego stało się niemożliwe z przyczyn leżących po stronie Oferenta.*" nie obejmują przypadku, w którym przedmiotowe działania wykonał inny wykonawca tworzący konsorcjum. Tak wniesione wadium należałoby zatem uznać za wadliwe, podzielając tym samy stanowisko zaprezentowane w analizowanym wyroku Krajowej Izby Odwoławczej.

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

Polecamy

SEMINARIUM
„TECHNOLOGICZNE, ORGANIZACYJNE I PRAWNE ASPEKTY CLOUD COMPUTINGU"
23 sierpnia 2011 r., Warszawa

W PROGRAMIE:
- Technologie Cloud Computing.
- Technologiczne perspektywy i ograniczenia rozwoju usług w modelu Cloud Computig.
- Aspekty organizacyjne usług Cloud Computing.
- Cloud Computing - wpływ na konkurencyjność przedsiębiorstw.
- Uwarunkowania bezpieczeństwa usług Cloud Computingu.
- Kryteria wyboru dostawcy usług w modelu Cloud Computingu.
- Prawne aspekty Cloud Computing.

Więcej: www.cpi.com.pl

cpi
centrum promocji informatyki

Zakończyła się XVI edycja Forum Informatyki w Administracji

Opracowanie:
Centrum Promocji Informatyki Sp. z o.o.

Już szesnasty raz, na zaproszenie Centrum Promocji Informatyki, przedstawiciele firm informatycznych oferujących technologie i rozwiązania niezbędne do tworzenia usług e-administracji spotkali się z przedstawicielami sektora publicznego. Tym razem dwudniowe forum wymiany informacji i wiedzy odbyło się w Mszczonowie. Do tradycji tej imprezy należy przeplatanie się prezentacji technicznych z przekazywaniem informacji o charakterze prawno-organizacyjnym. Bez rzetelnej wiedzy o zmieniających się regulacjach prawnych, związanych ze znowelizowaną ustawą o informatyzacji podmiotów realizujących zadania publiczne oraz nową ustawą o dowodach osobistych, trudno bowiem podejmować decyzje o kształcie tworzonych dla obywateli usług dostępnych drogą elektroniczną. Równie ważnym elementem dyskusji i prezentacji był też problem budowania systemów zarządzania informacją w urzędach administracji samorządowej i rządowej, a także archiwizowania i podejmowania decyzji o elektronicznym obiegu spraw w urzędzie. Pierwszy dzień forum prowadził Wiesław Paluszyński, wiceprezes Polskiego Towarzystwa Informatycznego.

Wstępem do dyskusji było bardzo ciekawe wystąpienie prof. Michała Kuleszy, który przedstawił uporządkowane relacje pomiędzy poszczególnymi obszarami administracji na tle obowiązujących regulacji ustrojowych państwa. Zwrócił uwagę na niepokojące tendencje do centralizacji zadań, sprzeczną z zasadami „zdolności do współdziałania", jaką powinna się cechować współpraca administracji rządowej z samorządową. Zdaniem Profesora, bez zlikwidowania tego, jak nazwał, „deficytu współdziałania" budowanie usług elektronicznych dla obywateli i komunikacji pomiędzy organami administracji będzie w dalszym ciągu ułomne.

Podniesiony przez prof. Kuleszę problem „stabilizacji kadrowej" kontynuował w swoim wystąpieniu Dagmir Długosz, zastępca Szefa Służby Cywilnej. Przedstawił on projekty, jakie są podejmowane w celu usprawnienia działania administracji i stabilizacji kadr. Na kanwie tej prezentacji wywiązała się ciekawa dyskusja dotycząca warunków, jakie powinny być spełnione, aby doprowadzić do stabilizacji kadr wśród specjalistów od technologii informacyjnych zatrudnionych w urzędach. Zwrócono uwagę na zasadniczy element dla tej stabilizacji, jakim powinien być wyraźny horyzont awansu w tej grupie specjalistów, połączony z awansem finansowym.

Kolejne wystąpienia były związane z prezentacją technologii i rozwiązań niezbędnych do tworzenia elektronicznego obiegu informacji w urzędzie. Podkreślono, że nie ma możliwości realizowania elektronicznych usług dla obywateli przez urząd niedysponujący narzędziami do elektronicznego obiegu spraw. Podstawą dla stworzenia takiego systemu jest właściwe zarządzanie infrastrukturą informatyczną urzędu.

Zdjęcie 1. Prof. Michał Kulesza

Możliwe rozwiązania przedstawił Michał Gawryś z IBM. Jego prezentacja, omawiająca koncepcję regionalnego centrum przetwarzania danych samorządowych, była mocno osadzona w realiach projektów, jakie realizuje administracja samorządowa w ramach programów dotowanych ze środków UE.

Kolejne wystąpienie - Wojciecha Mazurkiewicza z firmy EMC - dotyczyło sposobu wykorzystywania w projektowaniu systemów urzędów profesjonalnych metod zarządzania informacją i procesami biznesowymi. Kolejny raz podkreślono, że bez prawidłowego zdefiniowania procesów i dostępu do rejestrów referencyjnych i repozytoriów systemy e-usług nie mogą poprawnie działać.

W kolejnej prezentacji Wiesław Paluszyński, wiceprezes Polskiego Towarzystwa Informatycznego, przedstawił kwestie związane z nowym dowodem osobistym, który z założenia ma stać się kluczem do uwierzytelniania w systemach informatycznych sektora publicznego obywateli. Niestety, projekt ten jest znacznie opóźniony, a wobec zapowiedzi MSWiA o nowelizacji ustawy o dowodach osobistych może być zagrożony nie tylko czas udostępnienia tego narzędzia systemom informatycznym, ale także zakres udostępnionych funkcji. Biorąc pod uwagę, iż wiele systemów e-usług zakładało bazowanie na funkcjach DO przewidzianych w ustawie, może to spowodować znaczne problemy w działaniu większości systemów informatycznych zrealizowanych w ramach 7 osi POIG „Innowacyjna gospodarka". Zagrożenia te zostały omówione szczegółowo w trakcie prezentacji.

Kolejne prezentacje techniczne przedstawiały możliwości realizacji systemów obiegu informacji w urzędzie na przykładzie rozwiązań firmowych. I tak: o tym, jak wdrażać elektroniczny obieg dokumentów z wykorzystaniem narzędzi Share Point 2010, mówił Piotr Dąbrowski z firmy Passus. Jak migrować od pojedynczych funkcji e-urzędu do urzędu zintegrowanego prezentował Artur Siodmiak z firmy Otago. Janusz Szymura i Wojciech Sikora z firmy REKORD SI prezentowali sposób realizacji zintegrowanych usług w systemie RATUSZ.

O tym, jak ważne jest efektywne wykorzystywanie danych zbieranych przez elektroniczne systemy obiegu informacji w urzędach i roli w tym procesie systemów raportowania zarządczego, mówiła Małgorzata Szlachetka z Sygnity SA, a o aspektach interoperacyjności w budowaniu tych systemów - Krzysztof Kucz z tej samej firmy.

Rolę sprawnego zarządzania tworzeniem i udostępnianiem przez samorządy prawa miejscowego i narzędzia służące do realizacji tych funkcji prezentował Radosław Łukasik z Wolters Kulwers Polska.

Pierwszy dzień zakończyła oczekiwana przez wszystkich prezentacja Kazimierza Schmidta z MSWiA dotycząca problemów związanych z wdrażaniem instrukcji kancelaryjnej w wersji elektronicznej. Pomimo późnej pory problematyka ta wywołała ożywioną dyskusję.

Drugiego dnia obrady poprowadził Zbigniew Olejniczak, Dyrektor Centrum Projektów Informatycznych MSWiA. Tego dnia prezentacje dotyczyły przede wszystkim projektów realizowanych przez administrację centralną, których efekty są istotne dla budowy usług publicznych w jednostkach administracji samorządowej.

Wykład wprowadzający, autorstwa prof. Grażyny Szpor i Agnieszki Gryszczyńskiej z Uniwersytetu Kardynała Stefana Wyszyńskiego, dotyczył fundamentalnych problemów związanych z dokumentem elektronicznym i regulacjami prawnymi dotyczącymi tej problematyki w kontekście ryzyk, jakie są związane ze stosowaniem formy elektronicznej postępowań administracyjnych. Niestety, analiza ta pokazała, jak wiele jeszcze trzeba uporządkować w prawie, aby usługi elektroniczne mogły być skutecznie realizowane.

Kolejne prezentacje, Macieja Kaczmarka z Netgear mówiącego o bezpieczeństwie sieciowym w instytucjach publicznych i Artura Rutkowskiego z MCX Telecom 2 mówiącego o komunikacji w sytuacjach kryzysowych, były istotne ze względu na planowaną integrację centralnych systemów związanych z usługami ratownictwa.

Marek Sokołowski z ORACLE przekonywał, jak do celu budowy e-urzędu wykorzystywać produkty swojej firmy, a Mariusz Ferfecki z COIG prezentował wymianę informacji pomiędzy różnymi platformami zrealizowaną w projekcie Mdok.

Jedną z najważniejszych prezentacji tego dnia było przedstawienie przez Zbigniewa Olejniczaka stanu prac projektów realizowanych przez Centrum Projektów Informatycznych MSWiA.

Nową koncepcję Cyfrowej Łączności Dyspozytorskiej, jako ofertę komercyjną dla sektora publicznego, przedstawił Mariusz Chyliński z Polkomtel SA.

Forum zakończyła prezentacja Włodzimierza Marcińskiego, dyrektora departamentu Społeczeństwa Informacyjnego w MSWiA, poświęcona Europejskiej Agendzie Cyfrowej oraz Europejskiemu planowi działań na rzecz administracji do 2015 roku.

Niezależnie od ogromnego ładunku merytorycznego forum było jak zawsze okazją do wielu indywidualnych rozmów przy kolacji i kawie. A jak wiadomo, nic tak nie wspiera eliminacji własnych błędów, jak uczenie się od innych, dlatego takie spotkania są niezbędne i cieszą się znacznym zainteresowaniem uczestników. W tegorocznej edycji forum uczestniczyło około 150 osób.

Edwin Bendyk

Bohater naszych czasów

Bohaterem naszych czasów, niezmiennie od wielu lat, jest oczywiście Internet. Ostatnio z coraz większym zapałem jego znaczenie odkrywają politycy, na dobre i na złe, niestety. Weźmy prezydenta Francji Nicolasa Sarkozy'ego. Internet jest jego obsesją praktycznie od początku kadencji w Pałacu Elizejskim. Wielokrotnie wzywał, by w końcu zaprowadzić porządek w przestrzeni przypominającej, jego zdaniem, Dziki Zachód. Porządek, czyli uregulować cyberprzestrzeń zestawem praw, najlepiej o globalnym zasięgu.

Za krytyką internetowego ładu poszły czyny. Francja wprowadziła m.in. prawo Hadopi, mające uporządkować kwestię praw autorskich w domenie cyfrowej. Prawo Hadopi umożliwia odcinanie od Sieci złoczyńców, którzy obracają nielegalnymi treściami. Przestępca, niezależnie od innych sankcji przewidzianych w prawie karnym, skazywany jest na cyfrową banicję - specjalna czarna lista służy temu, żeby żaden dostawca usług nie ważył się sprzedać mu dostępu do Internetu. Instytucja zaiste średniowieczna, a analizy efektywności działania prawa Hadopi po pierwszym roku jego obowiązywania wykazały wiele ułomności. Jak jednak podkreślają złośliwi komentatorzy, wątpliwości nie mają żadnego znaczenia wobec siły producenckiego lobby, którego najskuteczniejszą agentką jest Carla Bruni. Tak się składa, że małżonka prezydenta.

W tym roku nadarzyła się okazja, by ambicjom regulacyjnego podboju Internetu nadać większy impet. Francja przewodniczy pracom grupy G8 skupiającej najważniejsze gospodarki świata. Nicolas Sarkozy wpadł więc na pomysł, by szczyt G8 poprzedzić międzynarodową konferencją poświęconą Internetowi. Na spotkanie e-G8 zjechali do Paryża najważniejsi (mierząc grubością portfeli) ludzie świata Sieci. Nie zabrakło Erika Schmidta z Google'a i Marka Zuckerberga z Facebooka. Ten ostatni w uznaniu doniosłości chwili i dla podkreślenia swojej dorosłości przywdział nawet garnitur i krawat. Zjechali wielcy świata reklamy, mediów i showbiznesu. Zabrakło dziwnym trafem przedstawicieli organizacji społecznych zajmujących się Internetem.

Rozpoczynając konferencję e-G8, prezydent Francji ponowił swoje postulaty, by poddać Internet ściślejszej kontroli. W odpowiedzi usłyszał, że specjalne regulacje nie są potrzebne, ważniejsze jest zaś zapewnienie powszechnego dostępu do Sieci każdemu obywatelowi świata. Przekonanie to wyrażali nie tylko ludzie internetowego biznesu, lecz także środowiska polityczne. David Cameron, premier Wielkiej Brytanii, dość uszczypliwie wyrażał się o pomysłach francuskiego kolegi. Na dodatek tuż przed konferencją e-G8 Brytyjczycy opublikowali raport o ochronie własności intelektualnej

opracowany na zamówienie Davida Camerona przez Iana Hargreavesa. Jego wymowa jest jednoznaczna - obowiązujące regulacje dotyczące własności intelektualnej, w tym system copyrightu, zamiast sprzyjać twórczości i innowacyjności, hamują rozwój.

Podobne zdanie wyrażał na konferencji e-G8 legendarny John Perly Barlow, niegdyś członek zespołu Grateful Dead, przekonujący, że prawo autorskie uformowane w zupełnie innej epoce nie odzwierciedla rzeczywistości Internetu. Artystyczne argumenty Barlowa w sposób bardziej systematyczny wyłożył Lawrence Lessig, amerykański prawnik i twórca inicjatywy Creative Commons. Stwierdził on, że nieprzemyślane regulacje służą zazwyczaj ochronie interesów firm zasiedziałych na rynku. Utrudniając wejście na rynek nowym, z konieczności bardziej innowacyjnym firmom, hamują nie tylko rozwój rynku, lecz także technologii i usług.

W sumie konferencja e-G8 nie doprowadziła do ważnych rozstrzygnięć. Sformowana na jej zakończenie sześcioosobowa delegacja powiozła do Deauville, na właściwy szczyt G-8 komunikat, że Internet jest dobry i należy starać się o jego upowszechnienie.

Bardziej zdecydowane stanowisko zajęły organizacje społeczne, które zorganizowały coś w rodzaju kontr-szczytu i wydały wspólne oświadczenie. Twierdzą w nim, że wolność Internetu jest poważnie zagrożona i to nie tylko w krajach niedemokratycznych. Również w demokracjach różnego typu regulacje w sposób bezpośredni lub pośredni grożą swobodzie komunikowania się. Przykładem nie tylko wspomniane francuskie prawo Hadopi, lecz także negocjowane w ramach Światowej Organizacji Handlu porozumienie ACTA o przeciwdziałaniu fałszerstwom. Porozumienie to, negocjowane w sposób całkowicie nieprzejrzysty (gdyby nie WikiLeaks, opinia publiczna nie poznałaby jego treści), pod szyldem porozumienia handlowego wprowadza w istocie możliwość kontroli obiegu informacji w Sieci.

Prezydent Francji odpowiada na zarzuty organizacji społecznych, że tylko wybrane w demokratycznych wyborach rządy dysponują legitymacją do wypowiadania się w imieniu społeczeństw. Ergo, jeśli prezydent Francji chce większej kontroli nad Internetem, to znaczy że w jego chceniu ucieleśnia się wola francuskiego ludu. Na szczęście wola ta nie obowiązuje w Polsce, gdzie póki co premier Donald Tusk reprezentuje mniej jakobińskie podejście do kwestii wyrażania woli ogólnej i chętnie ostatnio spotyka się z przedstawicielami organizacji społecznych zaangażowanych w sprawy Internetu. Czy skutkiem tych spotkań będą lepsze decyzje i mniej poronionych pomysłów, jak niesławna lista stron i usług niedozwolonych? Gwarancji nie ma, jest jednak szansa, którą warto wspierać.

Bibliografia zagadnień prawno-informatycznych 2010

Wojciech R. Wiewiórowski

Kedzierska Anna: *Digital signature in Poland – legal and technical aspects (selected issues)* [w:] Ewa Galwska [red.:] *European Information Law. Good Governance in the Public Sector*, CBKE 2010, s. 57-64

Kędzierski Jacek: *Ochrona prywatności i intymności w polskim prawie karnym - de lege ferenda,* „Palestra" 9-10/2010, s. 51-58

Kędzierski Marcin: *e-Zdrowie - fakty i mity*, „Czas Informacji" 4/2010

Kępczyński Robert: *E-administracja* [w:] Janusz Zawiła-Niedźwiedzki, Katarzyna Rostek, Artur Gąsiorkiewicz [red.:] *Informatyka gospodarcza. Tom 4*, C.H. Beck 2010

Kiełbus Maciej: *Dzienniki Ustaw odchodzą do lamusa*, „LexPress" 3/2010

Kiełtyka Leszek, Kucęba Robert: *Struktura przestrzeni informacyjnej w wirtualnym środowisku* [w:] Ryszard Borowiecki, Janusz Czekaj [red.:] *Zarządzanie zasobami informacyjnymi w warunkach nowej gospodarki,* Difin 2010

Kister Łukasz: *Audyt jako narzędzie oceny bezpieczeństwa informacji w organizacji* [w:] Małgorzata Gajos [red.:] *Ochrona informacji niejawnych, biznesowych i danych osobowych. Materiały z VI Kongresu*, Krajowe Stowarszyszenie Ochrony Informacji Niejawnych / Uniwersytet Śląski 2010, s. 57-62

Klafkowska-Waśniewska Katarzyna, Kępiński Jakub, Sikorski Rafał: *Ochrona zabezpieczeń technicznych a granice prawa autorskiego* [w:] Katarzyna Klafkowska-Waśniewska, Jakub Kępiński, Rafał Sikorski: *Granice prawa autorskiego. Tom 1*, C.H. Beck 2010

Klafkowska-Waśniewska Katarzyna, Kępiński Jakub, Sikorski Rafał: *Digital Rights Management Systems Systemy elektronicznego zarządzania prawami do utworów utrwalonych techniką cyfrową* [w:] Katarzyna Klafkowska-Waśniewska, Jakub Kępiński, Rafał Sikorski: *Granice prawa autorskiego. Tom 1*, C.H. Beck 2010

Klafkowska-Waśniewska Katarzyna, Kępiński Jakub, Sikorski Rafał: *Ewolucja wolnej licencji GNU General Public License v. 1.0, v. 2.0, v. 3.0* [w:] Katarzyna Klafkowska-Waśniewska, Jakub Kępiński, Rafał Sikorski: *Granice prawa autorskiego. Tom 1*, C.H. Beck 2010

Klafkowska-Waśniewska Katarzyna, Kępiński Jakub, Sikorski Rafał: *Dostosowywanie wersji 3.0 licencji Creatwe Commons do prawa polskiego - wybrane zagadnienia* [w:] Katarzyna Klafkowska-Waśniewska, Jakub Kępiński, Rafał Sikorski: *Granice prawa autorskiego. Tom 1*, C.H. Beck 2010

Klafkowska-Waśniewska Katarzyna, Kępiński Jakub, Sikorski Rafał: *Przesłanki odmowy udzielenia licencji wynikające z orzecznictwa do czasu sprawy Microsoft* [w:] Katarzyna Klafkowska-Waśniewska, Jakub Kępiński, Rafał Sikorski: *Granice prawa autorskiego. Tom 2*, C.H. Beck 2010

Klafkowska-Waśniewska Katarzyna, Kępiński Jakub, Sikorski Rafał: *Sprawa Microsoft – odmowa dostępu do informacji o interoperacyjności* [w:] Katarzyna Klafkowska-Waśniewska, Jakub Kępiński, Rafał Sikorski: *Granice prawa autorskiego. Tom 2*, C.H. Beck 2010

Klafkowska-Waśniewska Katarzyna, Kępiński Jakub, Sikorski Rafał: *Orzeczenie w sprawie Microsoft nową zasadą prawną?* [w:] Katarzyna Klafkowska-Waśniewska, Jakub Kępiński, Rafał Sikorski: *Granice prawa autorskiego. Tom 2*, C.H. Beck 2010

Klafkowska-Waśniewska Katarzyna, Kępiński Jakub, Sikorski Rafał: *Zakaz wiązania technologicznego z art. 102 TFUE (dawny art. 82 TWE) w świetle wyroku w sprawie Microsoft* [w:] Katarzyna Klafkowska-Waśniewska, Jakub Kępiński, Rafał Sikorski: *Granice prawa autorskiego. Tom 2*, C.H. Beck 2010

Klimowicz Marta: *Komunikacja internetowa na początku XXI wieku. Kultura indywidualizmu i narcyzm w mediach społecznych* [w:] Majka-Rostek Dorota [red.:] *Komunikacja społeczna a wyzwania współczesności*, Difin 2010

Kłak Marcin: *Zarządzanie wiedzą we współczesnym przedsiębiorstwie*, WSEIP Kielce 2010

Kociński Piotr: *Czy państwo potrzebuje architektury korporacyjnej?*, „Czas Informacji" 2/2010

Kociński Piotr: *Informatyzacja państwa rzymskiego a sprawa polska*, „Czas Informacji" 1/2010

Kociński Piotr: *Procesy - czy można je lekceważyć informatyzując państwo?,* „Czas Informacji" 3/2010

Kocot Wojciech J.: *Korzystanie z sieci teleinformatycznych w praktyce korporacyjnej spółek akcyjnych* [w:] Małgorzata Modrzejewska [red.:] *Prawo handlowe XXI wieku. Czas stabilizacji, ewolucji czy rewolucji. Księga jubileuszowa Profesora Józefa Okolskiego*, Wolters Kluwer 2010, s. 392-413

Koczkowski Mieczysław Tadeusz: *VI Kongres Ochrona informacji niejawnych, biznesowych i danych osobowych* [w:] Małgorzata Gajos [red.:] *Ochrona informacji niejawnych, biznesowych i danych osobowych. Materiały z VI Kongresu*, Krajowe Stowarzyszenie Ochrony Informacji Niejawnych / Uniwersytet Śląski 2010, s. 9-14

Kolczyński Janusz Piotr: *W sprawie niektórych autorskich praw osobistych pracownika do programu komputerowego oraz wyczerpania praw majątkowych on-line*, „Przegląd Prawa Handlowego" 1/2010, s. 36-43

Komorowski Krzysztof: *Dziesięć barier informatyzacji kraju*, „Czas Informacji" 1/2010

Konarski Konrad: *Elektroniczna komunikacja w zakresie postępowań podmiotów nadzorczych przy zwoływaniu posiedzeń i zgromadzeń w spółkach prawa handlowego*, „Czas Informacji" 1/2010

Kopka Bartosz: *System wieloagentowy jako narzędzie przetwarzania danych elektronicznych w jednostkach administracji publicznej* [w:] Jerzy Gołuchowski, Aldona Frączkiewicz-Wronka [red.:] *Technologie wiedzy w zarządzaniu publicznym*, Uniwersytet Ekonomiczny w Katowicach 2010

Korzeniowski Leszek F.: *Bezpieczeństwo informacyjne jako dobro społeczne* [w:] Małgorzata Gajos [red.:] *Ochrona informacji niejawnych, biznesowych i danych osobowych. Materiały z VI Kongresu*, Krajowe Stowarzyszenie Ochrony Informacji Niejawnych / Uniwersytet Śląski 2010, s. 63-76

Kos Maciej: *Użyteczność stron internetowych w e-biznesie* [w:] Jacek Winiarski [red.:] *Gospodarka elektroniczna współczesne przedsiębiorstwo na rynku globalnym*, Wydawnictwo Uniwersytetu Gdańskiego 2010

Kosiński Jerzy: *Hiszpańska propozycja zwalczania cyberprzestępczości* [w:] Agata Tyburska [red.:] *Ochrona infrastruktury krytycznej*, Wyższa Szkoła Policji w Szczytnie 2010

Kotarba Wiesław: *Ochrona własności intelektualnej w informatyce* [w:] Janusz Zawiła-Niedźwiedzki, Katarzyna Rostek, Artur Gąsiorkiewicz [red.:] *Informatyka gospodarcza. Tom 4*, C.H. Beck 2010

Kotecka Sylwia: *e-Temida oswojona*, „IT w Administracji" 2/2010

Kotecka Sylwia: *Informatyzacja postępowania cywilnego w Polsce* [w:] Jacek Gołaczyński [red:] *Informatyzacja postępowania sądowego i administracji publicznej,* C.H. Beck 2010

Kowalczuk Izabela: *Comparative questionnaire. Data protection* [w:] Ewa Galwska [red.:] *European Information Law. Good Governance in the Public Sector*, CBKE 2010, s. 111-122

Kowalska Ewa, Kowalski Mirosław: *Reklama w społeczeństwie informacyjnym,* Maternus Media 2010

Kowalski Jacek: *Działania z zakresu telekomunikacji, które mogą być podejmowane przez jednostki samorządu terytorialnego w celu zaspokajania zbiorowych potrzeb wspólnoty samorządowej*, „Czas Informacji" 3/2010

Kowalski Jacek: *Konsultacje UE na temat neutralności sieci*, „Czas Informacji" 4/2010

Kowalski Jacek: *Zasada neutralności sieci a relacje pomiędzy dostawcami kontentu i usług internetowych ISP*, „Czas Informacji" 2/2010

Krasińska Monika, Pilc Bogusława, Bałdyga Michał, Drobek Piotr, Kaczmarek Andrzej: *Systemy monitoringu audiowizualnego jako systemy przetwarzające dane osobowe* [w:] Małgorzata Gajos [red.:] *Ochrona informacji niejawnych, biznesowych i danych osobowych. Materiały z VI Kongresu*, Krajowe Stowarzyszenie Ochrony Informacji Niejawnych / Uniwersytet Śląski 2010, s. 77-92

Krasuski Andrzej: *Prawo telekomunikacyjne. Komentarz Wyd. III,* Lexis Nexis 2010

Krzemień Grzegorz: *Systemy zarządzania treścią w serwisach korporacyjnych* [w:] Witold Chmielarz, Tomasz Parys, Jerzy Kisielnicki [red:] *Informatyka w przyszłości*, Wydział Zarządzania Uniwersytetu Warszawskiego 2010

Krzykowska-Chmielewska Joanna: *Ochrona danych osobowych a system zarządzania bezpieczeństwem informacji wg normy PN-ISO/IEC 27001* [w:] Małgorzata Gajos [red.:] *Ochrona informacji niejawnych, biznesowych i danych osobowych. Materiały z VI Kongresu*, Krajowe Stowarzyszenie Ochrony Informacji Niejawnych / Uniwersytet Śląski 2010, s. 93-98

Krzysztofek Mariusz: *Ochrona danych osobowych osób fizycznych prowadzących działalność gospodarczą - glosa do wyroku Naczelnego Sądu Administracyjnego z 15.03.2010 r. I OSK 756/09,* „Glosa - Prawo Gospodarcze w Orzeczeniach i Komentarzach" 3/2010, s. 36-41

Krzysztofek Mariusz: *Tajemnica bankowa i ochrona danych osobowych w praktyce bankowej*, Lexis Nexis 2010

Kubiak Mariusz: *Wirtualne wojny epoki społeczeństwa informacyjnego* [w:] Małgorzata Gajos [red.:] *Ochrona informacji niejawnych, biznesowych i danych osobowych. Materiały z VI Kongresu*, Krajowe Stowarzyszenie Ochrony Informacji Niejawnych / Uniwersytet Śląski 2010, s. 99-108

Kubiak Przemysław: *Długofalowe bezpieczeństwo podpisu osobistego*, „Czas Informacji" 4/2010

Kudła Jacek: *Kontrola pracownika w ujęciu wybranych aspektów kontroli operacyjnej* [w:] Zbigniew Góral [red.:] *Kontrola pracownika możliwości techniczne i dylematy prawne,* Wolters Kluwer 2010

Kudrelek Jan: *Wykorzystanie zapisów z systemu monitoringu TV w postępowaniu karnym* [w:] Zbigniew Góral [red.:] *Kontrola pracownika możliwości techniczne i dylematy prawne,* Wolters Kluwer 2010

Kulesza Ewa: *Dopuszczalność kontroli pracowników w świetle przepisów o ochronie danych osobowych* [w:] Zbigniew Góral [red.:] *Kontrola pracownika możliwości techniczne i dylematy prawne,* Wolters Kluwer 2010

Kulesza Joanna: *Ius Internet. Między prawem a etyką*, WAIP 2010

Kulesza Joanna: *Międzynarodowe prawo internetu,* Ars Boni Et Aequi 2010

Kuliński Michał, *Regulacje komunikacji elektronicznej w rozwoju społeczeństwa informacyjnego w Unii Europejskiej,* C.H. Beck 2010

Kulisiewicz Tomasz: *Ile kosztuje podpis pod ustawą?*, „Czas Informacji" 3/2010

Kurowski Michał: *Procesowe wykorzystanie materiałów z kontroli pracownika - uwagi o możliwości wykorzystania niektórych dowodów prywatnych w procesie karnym* [w:] Zbigniew Góral [red.:] *Kontrola pracownika możliwości techniczne i dylematy prawne,* Wolters Kluwer 2010

Kuś Marcin: *Wpływ członkostwa Polski w NATO na kształtowanie polskiej polityki zagranicznej i jej bezpieczeństwa* [w:] Małgorzata Gajos [red.:] *Ochrona informacji niejawnych, biznesowych i danych osobowych. Materiały z VI Kongresu*, Krajowe Stowarzyszenie Ochrony Informacji Niejawnych / Uniwersytet Śląski 2010, s. 109-122

Kutyłowski Mirosław, Lauks-Dutka Anna: *Perspektywy rozwoju publicznych systemów elektronicznej identyfikacji* [w:] Jacek Gołaczyński [red:] *Informatyzacja postępowania sądowego i administracji publicznej,* C.H. Beck 2010

Kutyłowski Mirosław, Liu Yifan: *Prawo zamówień publicznych w Chinach*, „Czas Informacji" 3/2010

Kutyłowski Mirosław: *Ochrona bezpieczeństwa danych - granice wykorzystania podpisu elektronicznego*, „Czas Informacji" 1/2010

Kutyłowski Mirosław: *Pieczęć elektroniczna*, „Czas Informacji" 4/2010

Kuźnicka Aleksandra: *Egzekwowanie prawa autorskiego w Internecie a ochrona danych osobowych użytkowników, „*Zeszyty Naukowe Uniwersytetu Jagiellońskiego. Prace z Prawa Własności Intelektualnej" 110/2010

Kwaśnik Jakub: *Charakterystyka subkultury hackerów jako kluczowego elementu cyberprzestępczości,* „Internetowy Przegląd Prawniczy TBSP UJ" 1/2010, s. 24-39, http://www.tbsp.pl/upload/IPP4.pdf

Kwećka Roman: *Strategia bezpieczeństwa informacyjnego polistrategią bezpieczeństwa podmiotu* [w:] Piotr Sienkiewicz, Maciej Marszałek, Halina Świeboda [red.:] *Metodologia badań bezpieczeństwa narodowego. Bezpieczeństwo 2010. Tom 1,* Akademia Obrony Narodowej 2010

Kwiatkowska-Darul Violetta, Wójcikiewicz Józef: *Wartość diagnostyczna badania wariograficznego w stosunkach pracy* [w:] Zbigniew Góral [red.:] *Kontrola pracownika możliwości techniczne i dylematy prawne,* Wolters Kluwer 2010

Kwieciński Mirosław [red.] *Bezpieczeństwo informacji i biznesu zagadnienia wybrane*, Wydawnictwo Akademii F. Modrzewskiego 2010

Lach Arkadiusz: *Granice badań oskarżonego w celach dowodowych studium w świetle reguły nemo se ipsum accusare tenetur i prawa do prywatności*, TNOiK 2010

Lesiak Małgorzata: *Cases comparative session. Copyright and intellectual property* [w:] Ewa Galwska [red.:] *European Information Law. Good Governance in the Public Sector*, CBKE 2010, s. 123-136

Lesniak Marek: *Uwarunkowania prawne i metodyczne stosowania badań poligraficznych w sprawach zatrudnieniowych w Polsce* [w:] Małgorzata Gajos [red.:] *Ochrona informacji niejawnych, biznesowych i danych osobowych. Materiały z VI Kongresu*, Krajowe Stowarzyszenie Ochrony Informacji Niejawnych / Uniwersytet Śląski 2010, s. 123-132

Leszczak Oleg: *Podstawowe cechy społeczeństwa informacyjnego w aspekcie funkcjonalno-pragmatycznej teorii doświadczenia* [w:] Stefański Ryszard, Zamojski Adam [red.:] *Współczesny człowiek w społeczeństwie informacyjnym: egzystencja - ideologia – moralność*, Wydawnictwo Adam Marszałek 2010, s. 9-36

Leśniak Marek: *Informatyzacja postępowań rejestrowych w Krajowym Rejestrze Sądowym, Rejestrze Zastawów i Nowej Księdze Wieczystej oraz dostęp do danych zawartych w tych rejestrach* [w:] Jacek Gołaczyński [red:] *Informatyzacja postępowania sądowego i administracji publicznej,* C.H. Beck 2010

Levis Kieran: *Twórcy i ofiary ery Internetu*, Muza 2010

Lewandowska Hanna: *Technologie informatyczne w zarządzaniu podmiotami sektora ochrony zdrowia w wybranych krajach* [w:] Jerzy Gołuchowski, Aldona Frączkiewicz-Wronka [red.:] *Technologie wiedzy w zarządzaniu publicznym*, Uniwersytet Ekonomiczny w Katowicach 2010

Lewandowski Krzysztof: *Ochrona danych osobowych*, „Jurysta" 1/2010, s. 46-50

Lewandowski Krzysztof: *Przestępstwa przeciwko ochronie informacji w świetle rozdziału XXXXIII kodeksu karnego, orzecznictwa i doktryny,* „Wojskowy Przegląd Prawniczy" 3/2010, s. 61-76, http://lex.pl/czasopisma/wpp/art_3_10.pdf

Lichocki Ernest: *Cyberterroryzm a bezpieczeństwo teleinformatyczne Polski* [w:] Piotr Sienkiewicz, Maciej Marszałek, Halina Świeboda [red.:] *Metodologia badań bezpieczeństwa narodowego. Bezpieczeństwo 2010. Tom 1,* Akademia Obrony Narodowej 2010

Lichocki Ernest: *Ochrona krytycznej infrastruktury teleinformatycznej w aspekcie infrastruktury krytycznej państwa* [w:] Agata Tyburska [red.:] *Ochrona infrastruktury krytycznej*, Wyższa Szkoła Policji w Szczytnie 2010

Liedel Krzysztof: *Zarządzanie informacją w walce z terroryzmem*, Trio 2010

Łęcka Ewa: *Przekazywanie danych osobowych do państw trzecich* [w:] Tomasz Osiej, Jarosław Trelka [red.:] *Ochrona danych osobowych. Wybór zagadnień*, Omni Modo 2010

Łuczak Jacek, Tyburski Marcin: *Systemowe zarządzanie bezpieczeństwem informacji. ISO/IEC 27001,* Wydawnictwo Uniwerytetu Ekonomicznego w Poznaniu 2010

Łuczak Joanna: *Problematyka prawnych granic dopuszczalności kontroli poczty elektronicznej pracownika - rozważania na tle art. 267 k.k* [w:] Zbigniew Góral [red.:] *Kontrola pracownika możliwości techniczne i dylematy prawne,* Wolters Kluwer 2010

Łukaszewska Agata: *Dotacje na e-biznes. Pozyskiwanie środków z UE w ramach POIG 8.1,* OnePress 2010

Machała Wojciech: *Licencja mieszana? Prawnoautorskie aspekty obrotu programami komputerowymi stworzonymi z wykorzystaniem oprogramowania o otwartym kodzie. „*Zeszyty Naukowe Uniwersytetu Jagiellońskiego. Prace z Prawa Własności Intelektualnej" 107/2010, s. 28-37

Maciejuk Iwona: *Dopuszczalność dokonywania przez Generalnego Inspektora Ochrony Danych Osobowych oceny zgodności z prawem udostępnienia przez inne podmioty* [w:] Tomasz Osiej, Jarosław Trelka [red.:] *Ochrona danych osobowych. Wybór zagadnień*, Omni Modo 2010

Madejczyk Mariusz: *Zaufaj profilowi*, „IT w Administracji" 7/2010

Majchrowska Agata: *Odpowiedzialność odszkodowawcza z tytułu świadczenia usług elektronicznych z użyciem elektronicznych instrumentów płatniczych,* „Kwartalnik Naukowy - Prawo Mediów Elektronicznych" 1/2010, s. 25-30, http://cbke.prawo.uni.wroc.pl/files/pme/PME_1_2010.pdf

Majewski Jarosław: *Informacja objęta tajemnica bankową oraz informacja gospodarcza – różnice w poziomach ochrony* [w:] Krzysztof Markowski, Marek Wierzbowski [red.:] *Prawne uwarunkowania wymiany informacji – nowe wyzwania*, Stowarzyszenie Absolwentów WPiA UW 2009 [pozycja ukazała się jesienią 2010], s. 139-152

Malczewska Agnieszka: *Nadchodzi kontrola*, „IT w Administracji" 9/2010

Malczewska Agnieszka: *Oprogramowanie z drugiej ręki*, „IT w Administracji" 4/2010

Malý Jiři: *E-government in the Czech Republic: Essentials and possible developments* [w:] Ewa Galwska [red.:] *European Information Law. Good Governance in the Public Sector*, CBKE 2010, s. 137-144

Małecki Stanisław: *Ochrona informacji niejawnych (zarys wystąpienia podczas Kongresu)* [w:] Małgorzata Gajos [red.:] *Ochrona informacji niejawnych, biznesowych i danych osobowych. Materiały z VI Kongresu*, Krajowe Stowarzyszenie Ochrony Informacji Niejawnych / Uniwersytet Śląski 2010, s. 132-140

Małota Bogdan: *Działania korygujące i zapobiegawcze w zintegrowanych systemach zarządzania jakością i bezpieczeństwem informacji* [w:] Małgorzata Gajos [red.:] *Ochrona informacji niejawnych, biznesowych i danych osobowych. Materiały z VI Kongresu*, Krajowe Stowarzyszenie Ochrony Informacji Niejawnych / Uniwersytet Śląski 2010, s. 141-154

Mania Karolina: *ODR Online Dispute Resolution w sporach konsumenckich*, „ADR. Arbitraż i Mediacja" 2/2010, s. 15-22

Mania Karolina: *ODR Online Dispute Resolution w sporach konsumenckich*, „ADR. Arbitraż i Mediacja" 1/2010, s. 73-84

Mańka-Szulik Małgorzata: *Zastosowanie rozwiązań informatycznych w procesie komunikacji społecznej jednostki samorządu terytorialnego* [w:] Jerzy Gołuchowski, Aldona Frączkiewicz-Wronka [red.:] *Technologie wiedzy w zarządzaniu publicznym*, Uniwersytet Ekonomiczny w Katowicach 2010

Marcinkowska Joanna: *Roszczenie informacyjne w niemieckiej ustawie o prawie autorskim, „*Zeszyty Naukowe Uniwersytetu Jagiellońskiego. Prace z Prawa Własności Intelektualnej" 110/2010

Marcinkowska Edyta: *Czynniki społeczno-psychologiczne hamujące rozwój elektronicznej administracji w Polsce*, „Czas Informacji" 4/2010

Marciński Włodzimierz: *Wymiar Europejskiej Agendy Cyfrowej*, „Czas Informacji" 3/2010

Marek Jabłoński, Magdalena Mielus: *Zagrożenia bezpieczeństwa informacji w organizacji gospodarczej* [w:] Mirosław Kwieciński [red.] *Bezpieczeństwo informacji i biznesu zagadnienia wybrane,* Wydawnictwo Akademii F. Modrzewskiego 2010

Mariusz Rozwadowski: *Wykorzystanie metody SMED w procesie obsługi sprawcy wykroczenia drogowego* [w:] Mirosław Kwieciński [red.] *Bezpieczeństwo informacji i biznesu zagadnienia wybrane*, Wydawnictwo Akademii F. Modrzewskiego 2010

Mariusz Tchórzewski, Tomasz Telenga: *Elektroniczne postępowanie upominawcze. Komentarz,* Wolters Kluwer 2010

Markiewicz Joanna: *Prawo pracownika do prywatności w europejskim systemie ochrony praw człowieka* [w:] Zbigniew Góral [red.:] *Kontrola pracownika możliwości techniczne i dylematy prawne,* Wolters Kluwer 2010

Markowski Krzysztof, Wierzbowski Marek [red.:] *Prawne uwarunkowania wymiany informacji – nowe wyzwania*, Stowarzyszenie Absolwentów WPiA UW 2009 [pozycja ukazała się jesienią 2010]

Martinek Jacek: *Prowadzenie śledztwa w sprawach nielegalnego handlu paliwem z wykorzystaniem wspomagania informatycznego* [w:] Jacek Gołaczyński [red:] *Informatyzacja postępowania sądowego i administracji publicznej,* C.H. Beck 2010

Maruta Marcin: *Prawa autorskie w praktyce – klauzule, których brak, klauzule, których lepiej żeby nie było*, „Czas Informacji" 3/2010

Marzec Agnieszka: *System wymiany informacji o kredytobiorcach w świetle wyroku Europejskiego Trybunału Sprawiedliwości z dnia 23 listopada 2006 r. w sprawie C-238/05 Asnef-Equifax (Asnef) - (Ausbanc)* [w:] Krzysztof Markowski, Marek Wierzbowski [red.:] *Prawne uwarunkowania wymiany informacji – nowe wyzwania*, Stowarzyszenie Absolwentów WPiA UW 2009 [pozycja ukazała się jesienią 2010], s. 51-64

Masłowska Małgorzata, Naruszewicz Sylwia: *Informatyzacja procedur celnych,* Difin 2010

Maśko Łukasz, Żerański Paweł: *„Normalne korzystanie" z programów komputerowych przy świadczeniu usług finansowych i medialnych z użyciem systemów teleinformatycznych na tle europeizacji prawa polskiego, „*Zeszyty Naukowe Uniwersytetu Jagiellońskiego. Prace z Prawa Własności Intelektualnej" 107/2010, s. 38-65

Mateusz Kamiński: *Twój rejestr publiczny*, „IT w Administracji" 9/2010

Matlak Andrzej: *Dyrektywa o audiowizualnych usługach medialnych, „*Zeszyty Naukowe Uniwersytetu Jagiellońskiego. Prace z Prawa Własności Intelektualnej" 108/2010, s. 127

Matouk Kamal, *Portale e-learningowe jako element społeczeństwa informacyjnego*[w:] Iwona Chomiak-Orsa, Adam Nowicki, Henryk Sroka [red.:] *Informatyka ekonomiczna. Systemy informacyjne w zarządzaniu. Przegląd naukowo-dydaktyczny nr 17*, Wydawnictwo Uniwersytetu Ekonomicznego we Wrocławiu 2010, s. 126-136

Matusiewicz Krystian, Kutyłowski Mirosław: *Kryptograficzne funkcje skrótu - rzut oka na sytuację*, „Czas Informacji" 2/2010

Matuszak Justyna: *Legalność i adekwatność przetwarzania danych kadrowych* [w:] Tomasz Osiej, Jarosław Trelka [red.:] *Ochrona danych osobowych. Wybór zagadnień*, Omni Modo 2010

Mazur Magdalena: *Cyfryzacja coraz bliżej*, „IT w Administracji" 4/2010

Mazur Magdalena: *Dobro urzędowo osobiste*, „IT w Administracji" 1/2010

Mazur Magdalena: *Elektroniczny dowód osobisty*, „IT w Administracji" 10/2010

Mazur Magdalena: *Informacja przestrzenna*, „IT w Administracji" 12/2010

Mazur Magdalena: *Od jutra kable będą wszędzie*, „IT w Administracji" 8/2010

Mazur Magdalena: *Pakiet do zgryzienia*, „IT w Administracji" 2/2010

Mednis A.: *Ustawa o ochronie danych osobowych z perspektywy 10-lecia jej obowiązywania* [w:] Krzysztof Markowski, Marek Wierzbowski [red.:] *Prawne uwarunkowania wymiany informacji – nowe wyzwania*, Stowarzyszenie Absolwentów WPiA UW 2009 [pozycja ukazała się jesienią 2010], s. 153-164

Mencik Jaroslav: *Cases comparative session. Copyright and intellectual property* [w:] Ewa Galwska [red.:] *European Information Law. Good Governance in the Public Sector*, CBKE 2010, s. 145-154

Merklejn Iwona: *Teoria społeczeństwa informacyjnego Umesao Tadao i jej znaczenie dla dalszych badań* [w:] Francuz Piotr, Jędrzejewski Stanisław [red.:] *Nowe media i komunikowanie wizualne*, Wydawnictwo KUL 2010, s. 13-22

Michalak Arkadiusz: *Przegląd cywilnoprawnych instrumentów ochrony portali internetowych*, „Przegląd Prawa Handlowego" 4/2010, s. 19-24

Michalak Bartłomiej: *Proces informatyzacji niepublicznych zakładów opieki zdrowotnej - studium przypadku na przykładzie powiatu konińskiego* [w:] Jerzy Gołuchowski, Aldona Frączkiewicz-Wronka [red.:] *Technologie wiedzy w zarządzaniu publicznym*, Uniwersytet Ekonomiczny w Katowicach 2010

Miklus Magdalena: *Informacyjny wymiar procesu decyzyjnego organizacji gospodarczej* [w:] Ryszard Borowiecki, Janusz Czekaj [red.:] *Zarządzanie zasobami informacyjnymi w warunkach nowej gospodarki,* Difin 2010

Misztal-Konecka Joanna, Konecki Janusz, *Billing jako dowód w postępowaniu w sprawach o wykroczenia*, „Państwo i Prawo" 7/2010

Mitoraj Krzysztof: *Nie na wysypisko*, „IT w Administracji" 9/2010

Moroz Mirosław, *Innowacyjne sposoby przezwyciężania problemu „ostatniej mili" w e-commerce* [w:] Iwona Chomiak-Orsa, Adam Nowicki, Henryk Sroka [red.:] *Informatyka ekonomiczna. Systemy informacyjne w zarządzaniu. Przegląd naukowo-dydaktyczny nr 17,* Wydawnictwo Uniwersytetu Ekonomicznego we Wrocławiu 2010, s. 341-349

Mroczko Franciszek, Stańkowska Maria: *Informacja jako kluczowy zasób współczesnych organizacji* [w:] Ryszard Borowiecki, Janusz Czekaj [red.:] *Zarządzanie zasobami informacyjnymi w warunkach nowej gospodarki,* Difin 2010

Nacher Anna, Gorska-Olesińska Monika: *Bazy danych jako skrypty biograficzne – elektroniczny dyspozytyw pamięci*, „Opcje" 1/2010, s. 14-19

Najda-Janoszka Marta: *Organizacja wirtualna. Teoria i praktyka,* Difin 2010

Nasternak Aneta: *Biotechnologia jako problem społeczeństwa informacyjnego na przykładzie koncepcji „końca człowieka" Francisa Fukuyamy* [w:] Stefański Ryszard, Zamojski Adam [red.:] *Współczesny człowiek w społeczeństwie informacyjnym: egzystencja - ideologia – moralność*, Wydawnictwo Adam Marszałek 2010, s. 350-356

Nawrot Justyna: *Regulacyjny mechanizm interwencyjny w sektorze łączności elektronicznej,* „Gdańskie Studia Prawnicze" 22/2010, str. 157-178

Nazarek Wojciech: *Internet domains: Between law and technology – an Austrian dimension* [w:] Ewa Galwska [red.:] *European Information Law. Good Governance in the Public Sector*, CBKE 2010, s. 65-76

Niederliński Antoni: *Aplikacje prawno-administracyjne systemów ekspertowych* [w:] Jerzy Gołuchowski, Aldona Frączkiewicz-Wronka [red.:] *Technologie wiedzy w zarządzaniu publicznym*, Uniwersytet Ekonomiczny w Katowicach 2010

Nyczaj Krzysztof: *E-dokumentacja medyczna – idą zmiany*, „IT w Administracji" 8/2010

Nyczaj Krzysztof: *Rejestry a informacja publiczna*, „IT w Administracji" 7/2010

Obora Hubert: *Wybrane problemy pomiaru jakości informacji* [w:] Ryszard Borowiecki, Janusz Czekaj [red.:] *Zarządzanie zasobami informacyjnymi w warunkach nowej gospodarki,* Difin 2010

Okoń Zbigniew: *Modyfikacja i opracowanie programu komputerowego w polskim prawie autorskim,* „Zeszyty Naukowe Uniwersytetu Jagiellońskiego. Prace z Prawa Własności Intelektualnej" 110/2010

Okoń Zbigniew: *Programy komputerowe tworzone w ramach stosunku pracy*, „Kwartalnik Naukowy - Prawo Mediów Elektronicznych" 2/2010, s. 19-25 http://cbke.prawo.uni.wroc.pl/files/pme/PME_2_2010.pdf

Olszówka Kornelia, Ślęzak Andrzej: *Uwarunkowania tworzenia e-społeczności w otoczeniu placówki medycznej* [w:] Jerzy Gołuchowski, Aldona Frączkiewicz-Wronka [red.:] *Technologie wiedzy w zarządzaniu publicznym*, Uniwersytet Ekonomiczny w Katowicach 2010

Orłowski Jakub: *Cybersqatting,* „Edukacja Prawnicza" 10/2010, s. 36-40

Osiej Tomasz, Trelka Jarosław [red.:] *Ochrona danych osobowych. Wybór zagadnień*, Omni Modo 2010

Osiej Tomasz: *Portale społecznościowe a ochrona danych osobowych - wybrane zagadnienia* [w:] Tomasz Osiej, Jarosław Trelka [red.:] *Ochrona danych osobowych. Wybór zagadnień*, Omni Modo 2010

Osiej Tomasz: *Zbiory danych osobowych najczęściej zgłaszane do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych przez wybrane podmioty ze sfery administracji publicznej* [w:] Tomasz Osiej, Jarosław Trelka [red.:] *Ochrona danych osobowych. Wybór zagadnień*, Omni Modo 2010

Owoc Mieczysław L.: *Usability of Knowledge Grid In a Public Sector* [w:] Jerzy Gołuchowski, Aldona Frączkiewicz-Wronka [red.:] *Technologie wiedzy w zarządzaniu publicznym*, Uniwersytet Ekonomiczny w Katowicach 2010

Palikowska Katarzyna: *Portal Komunikacyjny Sądu PKS służący do elektronicznej komunikacji pomiędzy sądem a stronami postępowania* [w:] Jacek Gołaczyński [red:] *Informatyzacja postępowania sądowego i administracji publicznej,* C.H. Beck 2010

Panasiewicz Leszek: *Kulturowe uwarunkowania konkurencyjności opartej na informacji* [w:] Ryszard Borowiecki, Janusz Czekaj [red.:] *Zarządzanie zasobami informacyjnymi w warunkach nowej gospodarki,* Difin 2010

Pańkowska Małgorzata: *Model biznesowy przetwarzania rozproszonego cloud computing* [w:] Jerzy Gołuchowski, Aldona Frączkiewicz-Wronka [red.:] *Technologie wiedzy w zarządzaniu publicznym*, Uniwersytet Ekonomiczny w Katowicach 2010

Paszta Ewa: *Internet w działalności informacyjnej i komunikacyjnej przedsiębiorstw* [w:] Ryszard Borowiecki, Janusz Czekaj [red.:] *Zarządzanie zasobami informacyjnymi w warunkach nowej gospodarki,* Difin 2010

Paweł Waszkiewicz: *Wielki Brat Rok 2010. Systemy monitoringu wizyjnego - aspekty kryminalistyczne, kryminologiczne i prawne*, Wolters Kluwer 2010

Pawlik Kazimierz, Zenderowski Radosław: *Dyplom z internetu jak korzystać z internetu pisząc prace dyplomowe?*, CeDeWu 2010

Paź Włodzimierz: *Opis Projektu Rozwojowego „Kancelarie tajne"* [w:] Małgorzata Gajos [red.:] *Ochrona informacji niejawnych, biznesowych i danych osobowych. Materiały z VI Kongresu*, Krajowe Stowarzyszenie Ochrony Informacji Niejawnych / Uniwersytet Śląski 2010, s. 217-224

Pentor Research Int., FWiOO: *Wykorzystanie wolnego i otwartego oprogramowania w rządowej administracji publicznej. Raport z badania ilościowego dla Fundacji Wolnego i Otwartego oprogramowania – marzec 2010,* Fundacja Wolnego i Otwartego Oprogramowania 2010

Petzel Jacek: *Relewancja tekstów prawnych* [w:] Małgorzata Modrzejewska [red.:] *Prawo handlowe XXI wieku. Czas stabilizacji, ewolucji czy rewolucji. Księga jubileuszowa Profesora Józefa Okolskiego*, Wolters Kluwer 2010, s. 767-778

Piątek Zbigniew: *Telekomunikacyjna infrastruktura krytyczna w zarządzaniu kryzysowym* [w:] Agata Tyburska [red.:] *Ochrona infrastruktury krytycznej*, Wyższa Szkoła Policji w Szczytnie 2010

Piekarczyk Anna, Zimniewicz Kazimierz: *Myślenie sieciowe w teorii i praktyce,* PWE 2010

Pierzchała Krzysztof: *Keyword advertising - niewidzialne naruszenie prawa do znaku towarowego w Internecie? Analiza w świetle dyrektywy 2008/95/WE, „*Zeszyty Naukowe Uniwersytetu Jagiellońskiego. Prace z Prawa Własności Intelektualnej" 108/2010, s. 103-114

Pietras Agnieszka, Szczepańczyk Maciej: *Rola systemu informacyjnego instytucji wdrażających środki pomocowe UE dla przedsiębiorstw regionu łódzkiego* [w:] Ryszard Borowiecki, Janusz Czekaj [red.:] *Zarządzanie zasobami informacyjnymi w warunkach nowej gospodarki,* Difin 2010

Pietryka Artur: *Seminarium nt. "Stosowanie podsłuchów i kontroli operacyjnej a gwarancje praw i wolności jednostki - niezbędne zmiany prawne" (Warszawa, 16 listopada 2009 r.),* „Prokuratura i Prawo" 2/2011, s. 186-195

Pilich Mateusz: *Jeszcze o tzw. elektronicznych pismach procesowych w postępowaniu,* „Studia i Analizy Sądu Najwyższego" 4/2010

Podpłoński Robert: *Projekt ustawy o podpisach elektronicznych – wstęp do krytyki,* „Czas Informacji" 3/2010

Centrum Edukacji Medycznej CEMED

to nowoczesne centrum kształcenia kadry medycznej, organizator krajowych i międzynarodowych spotkań edukacyjnych

Dysponuje własnym **multimedialnym Centrum Konferencyjnym** z elastyczną możliwością konfiguracji pomieszczeń. Na blisko 500 m2 znajdują się 4 sale konferencyjne z naturalnym światłem, wyposażone w modułowe ściany przesuwne umożliwiające dostosowanie powierzchni do odpowiedniej liczby uczestników. Mogą one pomieścić od 35 do 170 osób. Wszystkie pomieszczenia są klimatyzowane i bardzo profesjonalnie wyposażone. Foyer konferencyjne o powierzchni 155 m2 pozwala na zorganizowanie wystawy i cateringu w bezpośrednim sąsiedztwie obrad. Do obsługi słuchaczy przygotowana jest profesjonalna recepcja z możliwością korzystania z niezbędnego sprzętu teleinformatycznego.

Profesjonalna reżyserka umożliwia kontrolę i zarządzanie **nowatorskimi systemami multimedialnymi** z jednego miejsca, z możliwością obserwacji całości imprezy. Centrum posiada:

- wyspecjalizowany system wideokonferencyjny umożliwiający połączenie z dowolnym miejscem na świecie w technologii HD,
- unikatowy system audio/video łączący sale konferencyjne z blokami operacyjnymi szpitala, umożliwiający uczestniczenie w operacji,
- system archiwizacji/nagrywania spotkań,
- obróbkę nagranego materiału audio/video,
- możliwość zorganizowania szkoleń z wykorzystaniem interaktywnego systemu Vote/PRS (Personal Response System).

Centrum Konferencyjne CEMED jest częścią kompleksu największego prywatnego szpitala ortopedycznego w Polsce (Carolina Medical Center), nasz nowatorski wyspecjalizowany system telekonferencyjny umożliwia przekaz na sale obrad obrazu z sal operacyjnych, gabinetów diagnostyki obrazowej, pomieszczeń fizjoterapii szpitala. Transmisji możemy dokonywać również z dowolnego punktu na świecie, dysponując urządzeniami o najlepszej jakości obrazu i dźwięku dostosowanymi do prezentacji medycznej treści edukacyjnej możemy transmitować np. obrazy RTG.

Dla organizatorów konferencji, szkoleń i imprez firmowych, menedżerów i prezesów firm szukających miejsc spotkań biznesowych Centrum Konferencyjne CEMED przedstawia ofertę wszechstronnych, fachowych usług według światowych standardów. Centrum położone jest w zacisznej części dolnego Mokotowa u zbiegu ulic Sikorskiego i Sobieskiego, tylko krok od centrum biznesowego i finansowego stolicy. Istotnym udogodnieniem Centrum jest duży parking poza strefą płatnego parkowania dostępny dla wszystkich gości.

Profesjonalna obsługa techniczna, jak i znakomita gastronomia gwarantują dobrą atmosferę towarzyszącą spotkaniom i konferencjom.
Wyjątkowe walory naszego centrum konferencyjnego sprawiają, że jesteśmy gotowi zorganizować najbardziej prestiżową konferencję, seminarium, szkolenie, jubileusz i galę.

Zapraszamy do skorzystania z naszych usług.

cemed
centrum edukacji medycznej

Karolina Sawczuk
Koordynator Centrum Konferencyjnego
tel. 22 355 85 05, kom. 501 312 496
e-mail: **k.sawczuk@cemed.pl**

Centrum Edukacji Medycznej CEMED Sp. z o.o.
ul. Pory 78, 02-757 Warszawa
www.cemed.pl

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 1/2011 - 4 kolejne numery		340 zł+5% VAT
prenumerata półroczna numer 1/2011 i 2/2011		200 zł+5% VAT

Prenumeratę prosimy przesłać do niżej wymienionego adresata

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

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

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

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

.....
pieczęć i podpis osoby upoważnionej

redaktor naczelny:	Wiesław Paluszyński wieslaw.paluszynski@czasinformacji.pl
kolegium redakcyjne:	Izabela Adamska, 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:	300 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.

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

wydawca:

cpi
centrum promocji informatyki

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.

centrum promocji informatyki

e-@dministracja
klub rozwoju technik informacyjnych

XVII FORUM INFORMATYKI W ADMINISTRACJI
ELEKTRONIZACJA PROCEDUR ADMINISTRACYJNYCH

5-6 października 2011 r., Hotel Warszawianka **** w Jachrance

Przez szesnaście kolejnych edycji Forum Informatyki w Administracji wykształciliśmy praktykę, która daje satysfakcjonujące rezultaty - stwarzamy uczestnikom Forum możliwość kształtowania (poprzez ankiety) programu następnej edycji. Dzięki temu uzyskujemy pewność, że agenda konferencji jest zbieżna z istotnymi dla tego środowiska problemami i odpowiada na najbardziej aktualne pytania.
Sukcesem przygotowań do kolejnej edycji Forum i potwierdzeniem rangi tej imprezy jest przyjęcie naszego zaproszenia przez Pana Wicepremiera Waldemara Pawlaka do wygłoszenia wykładu inaugurującego. Dwudniowy program został podzielony na pięć bloków tematycznych, co pozwoli na koncentrację obrad na szczególnie istotnych problemach. Mamy nadzieję, iż wzorem poprzednich edycji również obecna będzie dla Państwa interesującym i satysfakcjonującym spotkaniem.

Wybrane pozycje programu:
Uproszczenie i elektronizacja procedur administracyjnych
Przetwarzanie danych w e-administracji
Administracja w chmurze
Służby informatyczne w administracji - podnoszenie kwalifikacji
EZD w praktyce administracyjnej
Open Systems w administracji

Udział w programie potwierdzili m.in.:
dr hab. Paweł Fajgielski, kierownik Katedry Prawa Technologii Informacyjnych i Komunikacyjnych KUL
dr inż. Wacław Iszkowski, prezes Polskiej Izby Informatyki i Telekomunikacji
Rafał Malujda, ekspert wiodący ds. prawa Fundacji Wolnego i Otwartego Oprogramowania
Jerzy Nowak, Polskie Towarzystwo Informatyczne
Waldemar Pawlak, Wicepremier i Minister Gospodarki
Kazimierz Schmidt, Departament Społeczeństwa Informacyjnego MSWiA
prof. Grażyna Szpor, kierownik Katedry Prawa Informatycznego UKSW
dr Wojciech R. Wiewiórowski, GIODO oraz Uniwersytet Gdański, Wydział Prawa

www.e-administracja.org.pl/konferencje

Biuro organizacyjne:
Centrum Promocji Informatyki sp. z o.o.
ul. Międzyborska 50, 04-041 Warszawa
tel.: 22 870 69 78, faks: 22 870 69 95
email: cpi@cpi.com.pl