Paweł Krawczyk
ul. Miechowity 15/19
31-475 Kraków
Tel. 602-776959
Email pawel.krawczyk@hush.com

Kraków, 2011-2-16

Uwagi do projektu rozporządzenia Krajowe Ramy Interoperacyjności z dnia 10 lutego 2011

Szanowni Państwo,

Przekazuję uwagi do projektu rozporządzenia Rady Ministrów w sprawie Krajowych Ram Interoperacyjności opublikowanego w BIP MSWiA w dniu 10 lutego 2011.

Uwaga 1.

Projekt niezbyt precyzyjnie określa zakres stosowania poszczególnych wymagań technicznych, przez co niektóre z nich mogą skutkować zamieszaniem lub być w praktyce ignorowane, podobnie jak w przypadku poprzedniego rozporządzenia o minimalnych wymaganiach.

Na przykład **§ 11** wprowadza zasadę, że *„kodowanie znaków odbywa się według standardu Unicode UTF-8”*, przy czym nie do końca wiadomo o jakie znaki chodzi – czy chodzi o wszystkie dokumenty przetwarzane przez administrację?

Tak rozumiany wymóg będzie w praktyce niemożliwy do zrealizowania oraz nieuzasadniony. Kodowanie znaków jest kwestią wtórną i jedną z wielu (struktura, formatowanie). Unifikacja kodowania w nowych systemach może być korzystna, ale prowadzona na zasadzie „urawniłowki” wyrządzi więcej szkód niż korzyści.

Zalecenie: uporządkowanie kwestii formatów stosowanych w administracji przez wskazanie obligatoryjnych oraz zalecanych list formatów do konkretnych zastosowań, a nie „do wszystkiego” (patrz dalej).

Uwaga 2.

***„§ 12. 1**. Jeżeli dla pisma w formie dokumentu elektronicznego służącego do procedowania danej sprawy nie ustalono wzoru dokumentu elektronicznego”*

Czy w ustawie o informatyzacji lub KPA istnieje jakiś przepis nakładający na jednostki administracji publicznej obowiązek tworzenia i publikowania takich wzorów? Jeśli nie, to przepis ten stanie się szybko furtką niespójne, lokalnie opracowane rozwiązania, sankcjonowane istnieniem jakiegoś „darmowego programu umożliwiającego odczytanie”, niezależnie od jego niekompatybilności z innymi rozwiązaniami.

Uwaga 3.

„§11. 2. 4) *Kodowanie znaków odbywa się według standardu Unicode UTF-8”*

Po pierwsze, ten niskopoziomowy i techniczny wymóg jest umieszczony wśród listy organizacji normalizacyjnych (IETF i W3C), przez co staje się niezrozumiały. O kodowanie jakich znaków chodzi? W obecnej formie można pomyśleć, że chodzi o kodowanie znaków w wymienionych normach i standardach.

Po drugie, formatowanie tego akapitu również nie poprawia jego czytelności. Paragraf 11, ustęp 2 kończy się na poprzedniej stronie listą punktów numerowanych 1) i 2). Na następnej stronie kontynuowane są punkty z numeracją właściwą dla ustępów (3., 4.) ale z wcięciem sugerującym, że są one częścią ustępu 2.

Po trzecie, wymóg kodowania wszystkich znaków w UTF-8 jest po pierwsze nierealny, po drugie szkodliwy. Jak pisałem powyżej, kodowanie znaków to kwestia wtórna. W administracji publicznej stosowane są liczne kodowania, będące pozostałością z przeszłości (np. w systemie POLTAX czy innych budowanych w latach 80. lub 90.). Ich wykorzystanie wewnątrz systemów nie stanowi problemu, a w razie potrzeby eksportu danych można je przekodować.

Zalecenie: kodowanie w UTF-8 powinno mieć charakter **zalecenia** w stosunku do nowobudowanych systemów i powinno być umieszczone w części technicznej KRI (załącznik nr 2). Równocześnie KRI powinny precyzyjnie określać zakres obowiązywania poszczególnych wymagań (patrz dalej).

Uwaga 4.

Z brzmienia **§15** wynika, że rozliczalność w systemach teleinformatycznych powinna dotyczyć tylko ograniczonego zbioru czynności (ust. 2, pkt 1-3) – w szczególności dostępu z prawami administratora oraz *"działań użytkowników lub procesów polegających na dostępie do (...) przetwarzanych w systemach danych podlegających prawnej ochronie"*.

Przepis ten jest niejasny. O jaką „prawną ochronę” chodzi? W obecnej postaci należy rozumieć go w ten sposób, że o ile nie jest to nakazane odrębnymi przepisami, to np. system obiegu dokumentów czy pracy grupowej **nie musi w ogóle odnotowywać, że dana osoba odczytała dany dokument lub wprowadziła do niego zmiany**.

Jest to poważna luka, ponieważ brak rejestru operacji dokonywanych przez zwykłych użytkowników będzie oznaczał brak możliwości zabezpieczenia materiału dowodowego w razie podejrzenia przestępstwa (jak w przypadku słynnego fragmentu „...lub czasopisma” czy paragrafu 428 prawa górniczego).

Zalecenie: rejestry systemowe powinny, zgodnie z punktem A.10.10.1 normy PN ISO/IEC 27001, rejestrować także aktywność użytkowników systemu, niezależnie od aktywności administratorów (A.10.10.4).

Uwaga 5.

Projekt KRI pomija kwestie własności majątkowych praw autorskich oraz licencji na systemy zamawiane przez jednostki administracji publicznej. Mają one kluczowe znaczenie dla interoperacyjności oraz efektywności finansowej, administracji

Częste są sytuacje gdy kilka jednostek administracji pełniących tę samą rolę i działających na podstawie tych samych przepisów (np. sądy, urzędy wojewódzkie itd.) zleca na zewnątrz kompleksową usługę polegającą na opisaniu procesów administracyjnych, napisaniu systemu oraz jego wdrożeniu.

W rzeczywistości tylko ostatni krok (dostosowanie i wdrożenie) jest specyficzny dla danego urzędu, w pozostałych urzędy wielokrotnie wydają pieniądze na opisywanie tych samych procesów i pisanie tych samych systemów.

Krajowe Ramy Interoperacyjności powinny wprost określać właściwy sposób postępowania w takich przypadkach – to znaczy jednostka sporządzająca np. opis procesów po raz pierwszy może zamówić go z przekazaniem całości majątkowych praw autorskich, a następnie nieodpłatnie udostępnić pozostałym urzędom w analogicznej sytuacji. Ministerstwo właściwe do spraw informatyzacji mogłoby także koordynować bazę takich opracowań.

Uwaga 6.

Załącznik nr 2 do projektu rozporządzenia zawiera praktycznie tę samą treść, co poprzednio obowiązujące rozporządzenie o minimalnych wymaganiach.

§ 12. Ust. 2 mówi, że *„systemy teleinformatyczne podmiotów realizujących zadania publiczne powinny udostępniać zasoby informacyjne co najmniej w jednym z formatów plików określonych w załączniku nr 2”*. Sformułowanie „udostępniać” jest niejasne i będzie z pewności skutkować wątpliwościami interpretacyjnymi. Systemy mogą bowiem „udostępniać” dane w co najmniej kilku kontekstach:

1. Udostępniać je innym modułom danego systemu (np. komunikacja między serwerem aplikacji i bazą danych)
2. Udostępniać je systemom innych podmiotów publicznych (np. wymiana między systemami ZUS, PIP i NFZ, *government to government*, G2G)
3. Udostępniać je obywatelom (*government to citizen*, G2C).

W każdym z tych przypadków potrzeby funkcjonalne wobec stosowanych formatów są całkowicie odmienne i ich ujednolicenie metodą „jeden rozmiar dla wszystkich” spowoduje więcej szkody niż pożytku. W szczególności:

1. W komunikacji wewnątrz systemów, lub nawet między jednostkami administracji (G2G) stosowanie formatów prywatnych i niestandardowych może być uzasadnione wydajnością czy innymi szczególnymi potrzebami. Dla właściciela lub licencjobiorcy jest natomiast uniknięcie uzależnienia technologicznego (*vendor lock-in*) polegającego na tym, że jego dane zostaną nieodwracalnie zapisane w prywatnym, nieudokumentowanym formacie, bez możliwości eksportu czy konwersji.
    a. W obecnym brzmieniu projektu „nielegalne” staną się wszystkie formaty komunikacji tego typu (na przykład DER). Co więcej, bezcelowe (i praktycznie niemożliwe) jest wyliczenie wszystkich stosowanych w informatyce formatów.
    b. **Zalecenie**: w odniesieniu do wymiany danych wewnątrz systemu, każdy logiczny moduł powinien mieć możliwość eksportu danych do standardowego lub udokumentowanego formatu. W ten sposób możliwe będzie zastąpienie jednego modułu innym bez utraty przechowywanych w nim danych.
2. W komunikacji G2G istotne jest nie tyle stosowanie formatów wymienionych w załączniku nr 2, tylko spowodowanie by stosowane formaty były poprawnie udokumentowane. Interoperacyjność pomiędzy systemami różnych urzędów jest prawdopodobnie najistotniejszym elementem KRI.
    a. **Zalecenie**: jednostki administracji powinny posiadać co najmniej dostęp do specyfikacji protokołu czy formatu stosowanych do wymiany informacji między systemami, a w

przypadku systemów zamawianych na swój wyłączny użytek – także majątkowe prawa autorskie do specyfikacji i implementacji.

b. **Zalecenie**: komunikacja między systemami powinna być oparta o standardowy i otwarty interfejs (np. SOAP w przypadku usług webowych), a nowe systemy powinny być z takimi interfejsami zamawiane. Umożliwi to łączenie systemów różnych podmiotów ze sobą bez potrzeby ich modyfikacji.

3. Formaty dokumentów udostępniane obywatelom powinny być jak uregulowane najściślej ze względu na dużą liczbę dostępnych na rynku programów klienckich i systemów operacyjnych. Stosowanie standardowych formatów w określonej wersji maksymalnej (a nie minimalnej jak dotąd) zapewni, że każdy obywatel będzie mógł komunikować się z administracją przy użyciu ogólnodostępnych narzędzi.
    a. **Zalecenie**: lista powinna określać minimalne i **maksymalne** wersje formatów dopuszczalnych w danym momencie z uwzględnieniem jego rozpowszechnienia wśród klientów. Lista taka powinna mieć charakter kroczący, aktualizowany co najmniej co 2-3 lata.
        i. Np. format PDF w wersjach od 1.3 do 1.7, co wyeliminowałoby niestandardowe rozszerzenia Adobe, w przeciwnym razie dopuszczalne przez ogólne sformułowanie „format PDF".
    b. **Zalecenie**: Lista powinna dopuszczać wyłącznie formaty, którymi zarządzają organizacje normalizacyjne i odwoływać się do konkretnych norm.
        i. Np. w przypadku formatu PDF byłaby to norma ISO 32000. Z listy powinny zdecydowanie zniknąć formaty RAR, TAR czy GZIP. Są to formaty specjalistyczne, które nie powinny być używane do udostępniania czegokolwiek obywatelom. Równocześnie nic nie stoi na przeszkodzie by stosować je wewnątrz systemów czy w komunikacji G2G, jeśli spełnią warunek dostępności specyfikacji.
    c. **Zalecenie**: Tam gdzie to uzasadnione, KRI powinny określać konkretny wariant lub profil formatu, których może być wiele (np. PDF czy XAdES).
        i. Np. w przypadku formatu PDF określić należy wariant (np. PDF/A), kodowanie znaków (UTF-8) oraz osadzenie treści w postaci tekstu a nie zeskanowanego obrazu.

Obecna postać załącznika nr 2 jest – podobnie jak oryginalne rozporządzenie z 2005 roku – dość chaotyczna i zawiera wiele luk. Między innymi:

- Nie są wymienione konkretne normy i standardy definiujące wymienione, nawet te, które są już normami ISO (PDF, ODT).
- Jako organizacje zarządzające są wymienione prywatne firmy, które stworzyły dany format, nawet w tych przypadkach, gdy od dawna formatem zarządzają organizacje takie jak ISO, OASIS czy ECMA.
- Wymienione są formaty niszowe i specjalistyczne (TAR, GZIP) lub prywatne, funkcjonujące wyłącznie na zasadzie standardu de facto (RAR). Równocześnie brak jest – jeśli już trzymalibyśmy się logiki katalogu formatów – popularnych formatów arkuszy kalkulacyjnych (XLS, XLSX, ODS).
- W projekcie rozporządzenia zupełnie pominięte zostały protokoły komunikacyjne, które przecież z punktu widzenia interoperacyjności mogą być równie kłopotliwe jak formaty danych. Czy np. w rozumieniu rozporządzenia protokół SSL jest „standardem"? Jeśli tak, to należy go uznać za niezgodny
- Poza protokołami pominięto cały szereg formatów mniej znanych i mniej wyeksponowanych, ale powszechnie wykorzystywanych – na przykład format DER, używany do zapisywania certyfikatów X.509.

Z poważaniem, Paweł Krawczyk