Projekt kierowany do akceptacji

ROZPORZĄDZENIE
RADY MINISTRÓW

z dnia …… 2011 r.

w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w formie elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych

Na podstawie art. 18 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. Nr 64, poz. 565, z późn. zm. [1)]) zarządza się, co następuje:

§ 1. Rozporządzenie określa:

1) Krajowe Ramy Interoperacyjności;
2) minimalne wymagania dla rejestrów publicznych i wymiany informacji w formie elektronicznej;
3) minimalne wymagania dla systemów teleinformatycznych, w tym:
   a) specyfikację formatów danych oraz protokołów komunikacyjnych i szyfrujących, które mają być stosowane w oprogramowaniu interfejsowym,
   b) sposoby zapewnienia bezpieczeństwa przy wymianie informacji,
   c) standardy techniczne zapewniające wymianę informacji z udziałem podmiotów publicznych z uwzględnieniem wymiany transgranicznej,
   d) sposób zapewnienia dostępu do treści prezentowanych przez podmioty publiczne dla osób niepełnosprawnych.

§ 2. Terminy użyte w rozporządzeniu oznaczają:

1) aktywa – wszystko, co ma wartość dla podmiotu, inaczej zasoby;
2) architektura systemu teleinformatycznego – opis ogółu składników systemu teleinformatycznego, powiązań i relacji pomiędzy tymi składnikami oraz procesów przebiegające w systemie;
3) autentyczność – właściwość zapewniająca, że tożsamość podmiotu lub zasobu jest taka, jak deklarowana;
4) dostępność – właściwość bycia dostępnym i użytecznym na żądanie upoważnionego podmiotu;
5) integralność – właściwość polegająca na zapewnieniu dokładności i kompletności aktywów;
6) interesariusz – osobę lub podmiot posiadający interes prawny albo faktyczny w sprawach interoperacyjności;
7) model architektury – formalny opis architektury systemu teleinformatycznego;
8) model usługowy – model architektury, w którym zdefiniowano określone funkcje systemu teleinformatycznego stanowiące odrębną całość, dostępne dla użytkowników oraz opis sposobu korzystania z tych funkcji;

[1)] zmiany wymienionej ustawy zostały ogłoszone w Dz. U. z 2006 r. Nr 12, poz. 65 i Nr 73, poz. 501, z 2008 r. Nr 127, poz. 817, z 2009 r. Nr 157, poz. 1241 oraz z 2010 r. Nr 40, poz. 230, Nr 167 poz. 1131 i Nr 182, poz. 1228.

9) nieodpłatne oprogramowanie – oprogramowanie udostępniane przez właściciela autorskich praw majątkowych bez pobierania opłaty za jego użytkowanie na warunkach określonych przez tego właściciela;
10) niezaprzeczalność – brak możliwości wyparcia się swego uczestnictwa w całości lub w części wymiany danych przez uczestnika tej wymiany;
11) obiekt – przedmiot opisu w rejestrze publicznym;
12) obiekt przestrzenny – abstrakcyjną reprezentację przedmiotu, zjawiska fizycznego lub zdarzenia związanego z określonym miejscem lub obszarem geograficznym;
13) podatność systemu teleinformatycznego – właściwość systemu teleinformatycznego, która może być wykorzystana przez co najmniej jedno zagrożenie;
14) podmiot – osobę prawną, jednostkę organizacyjną nie posiadającą osobowości prawnej albo organ administracji publicznej;
15) poufność – właściwość, że informacja nie jest udostępniana lub wyjawiana nieupoważnionym osobom fizycznym, podmiotom lub procesom;
16) repozytorium rekomendacji interoperacyjności – adres internetowy na ePUAP, pod którym udostępnia się, do zapoznania lub pobrania, rekomendacje interoperacyjności;
17) rozliczalność – właściwość zapewniająca, że działania osoby fizycznej, podmiotu lub procesu mogą być przypisywane w sposób jednoznaczny tylko tej osobie fizycznej, podmiotowi lub procesowi;
18) ustawa – ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne;
19) wzór dokumentu elektronicznego – wzór, o którym mowa w art. 19b ustawy;
20) zagrożenie systemu teleinformatycznego – potencjalna przyczyna niepożądanego zdarzenia, która może wywołać szkodę w systemie teleinformatycznym.

§ 3. 1. Krajowe Ramy Interoperacyjności stanowią zbiór uzgodnionych definicji, wymagań, reguł architektury systemów teleinformatycznych oraz procedur i zasad, których stosowanie umożliwi współdziałanie systemów teleinformatycznych podmiotów realizujących zadania publiczne w procesach realizacji tych zadań drogą elektroniczną.

2. Krajowe Ramy Interoperacyjności określają w szczególności:

1) sposoby postępowania podmiotu realizującego zadania publiczne w zakresie doboru środków, metod i standardów wykorzystywanych do ustanowienia, wdrożenia, eksploatacji, monitorowania, przeglądu, utrzymania i udoskonalania systemu teleinformatycznego wykorzystywanego do realizacji zadań tego podmiotu oraz procedur organizacyjnych, mające na celu:
   a) zapewnienie obywatelom oraz podmiotom gospodarczym, dostępności usług publicznych, w postaci elektronicznej,
   b) zwiększenie efektywności usług świadczonych przez administrację publiczną,

c) zapewnienie obywatelom i podmiotom gospodarczym zmniejszenia obciążeń związanych z realizacją uprawnień i obowiązków przewidzianych w przepisach odrębnych,

d) zapewnienie podmiotom publicznym redukcji kosztów funkcjonowania,

e) zapewnienie racjonalnego gospodarowania funduszami publicznym,

f) zapewnienie swobody gospodarczej i równego dostępu do rynku informatycznego dla wszystkich jego uczestników w zakresie zamówień publicznych realizowanych przez podmioty realizujące zadania publiczne w zakresie systemów teleinformatycznych;

2) obowiązki ministra właściwego do spraw informatyzacji w zakresie przejrzystego określenia sposobu wyboru norm, standardów i rekomendacji w zakresie interoperacyjności semantycznej, organizacyjnej oraz technologicznej, z zapewnieniem zasady równego traktowania różnych rozwiązań informatycznych.

3. Na Krajowe Ramy Interoperacyjności składają się w szczególności:

1) architektura systemów teleinformatycznych podmiotów realizujących zadania publiczne;

2) sposób osiągania interoperacyjności;

3) repozytorium rekomendacji interoperacyjności na ePUAP.

§ 4. 1. Interoperacyjność osiąga się poprzez:

1) ujednolicenie, rozumiane jako zastosowanie tego samego typu sprzętu, oprogramowania, tych samych standardów, polityk, procedur i norm przez różne podmioty realizujące zadania publiczne;

2) wymienność, rozumianą w ten sposób, że jeden produkt, proces lub usługa mogą być zastąpione innymi bez zakłócenia wymiany informacji pomiędzy podmiotami realizującymi zadania publiczne lub pomiędzy tymi podmiotami a ich klientami, przy jednoczesnym spełnieniu wszystkich wymagań funkcjonalnych i pozafunkcjonalnych współpracujących systemów;

3) zgodność, rozumianą jako przydatność produktów, procesów lub usług przeznaczonych do wspólnego użytkowania, pod specyficznymi warunkami zapewniającymi spełnienie istotnych wymagań i przy braku niepożądanych oddziaływań.

2. Sposób osiągania interoperacyjności poprzez zastosowanie reguł określonych w ust. 1 powinien być zależny od okoliczności wynikających z szacowania ryzyka oraz z właściwości projektowanego systemu teleinformatycznego, jego zasięgu oraz dostępnych rozwiązań na rynku dostaw i usług w zakresie informatyki.

3. Zastosowany przez podmiot publiczny realizujący zadania publiczne sposób osiągnięcia interoperacyjności nie może naruszać zasady równego traktowania różnych rozwiązań informatycznych.

§ 5. 1. Podmioty realizujące zadania publiczne stosują rozwiązania z zakresu interoperacyjności na poziomie organizacyjnym, semantycznym i technologicznym.

2. Interoperacyjność na poziomie organizacyjnym osiągana jest w szczególności przez:

1) informowanie przez podmioty realizujące zadania publiczne o sposobie dostępu oraz zakresie użytkowym serwisów usług realizowanych przez te podmioty;

2) wskazanie przez ministra właściwego do spraw informatyzacji miejsca przeznaczonego do publikacji informacji o których mowa w pkt 1;

3) stosowanie przez podmioty realizujące zadania publiczne, uzgodnionych i opublikowanych na ePUAP przez ministra właściwego do spraw informatyzacji, rekomendacji dotyczących rozwiązań na poziomie semantycznym i technologicznym, innych niż wynikające z obowiązujących przepisów prawa, wypracowanych w jawnym i otwartym procesie uzgodnień z możliwie szerokim gronem interesariuszy;
4) standaryzację i ujednolicenie procedur z uwzględnieniem potrzeb wynikających z informatyzacji podmiotu;
5) publikowanie i uaktualnianie przez podmiot realizujący zadania publiczne, w Biuletynie Informacji Publicznej, opisów procedur obowiązujących przy załatwianiu spraw na drodze elektronicznej z zakresu jego właściwości.

3. Interoperacyjność na poziomie semantycznym osiągana jest w szczególności przez:
1) stosowanie struktur danych i znaczenia danych zawartych w tych strukturach, określonych w niniejszym rozporządzeniu oraz w rekomendacjach ministra właściwego do spraw informatyzacji publikowanych na ePUAP;
2) stosowanie w rejestrach prowadzonych przez podmioty publiczne odwołań w zakresie niezbędnym do realizacji zadań do rejestrów zawierających dane referencyjne.

4. Interoperacyjność na poziomie technologicznym osiągana jest w szczególności poprzez:
1) stosowanie rozwiązań zawartych w przepisach § 10 – 14;
2) stosowanie odrębnych regulacji, a w przypadku ich braku norm krajowych, norm Unii Europejskiej, norm międzynarodowych, a także rekomendacji publikowanych przez ministra właściwego do spraw informatyzacji lub standardów uznanych w drodze dobrej praktyki przez organizacje międzynarodowe.

§ 6. 1. Projektując system teleinformatyczny służący do realizacji zadań publicznych należy przyjąć rozwiązania oparte na modelu usługowym.

2. W przypadkach uzasadnionych specyfiką systemu dopuszcza się inny model architektury.

§ 7. 1. Organem właściwym dla zapewnienia warunków do osiągania interoperacyjności na szczeblu krajowym jest minister właściwy do spraw informatyzacji.

2. Organ wskazany w ust. 1 odpowiada za:
1) umożliwienie publicznej dyskusji nad rekomendacjami interoperacyjności z zachowaniem zasady neutralności technologicznej i otwartości standardów oraz zgodności z normami zatwierdzonymi przez krajową jednostkę normalizacyjną lub normami i standardami rekomendowanymi lub ustalanymi jako obowiązujące przez organy Unii Europejskiej;
2) prowadzenie repozytorium rekomendacji interoperacyjności.

§ 8. 1. W rejestrach publicznych mogą być wyróżnione w szczególności następujące typy obiektów:
1) osoba fizyczna posiadająca nadany numer PESEL;
2) podmiot;
3) obiekt przestrzenny.

2. Dla każdego obiektu, o którym mowa w ust. 1, w obrębie danego typu, nadaje się unikatowy identyfikator.

3. Rodzaje identyfikatorów oraz ich strukturę określa załącznik nr 1 do rozporządzenia.

4. Podmioty realizujące zadania publiczne z wykorzystaniem wymiany informacji za pomocą teletransmisji danych lub za pomocą pism w formie dokumentów elektronicznych sporządzonych według wzorów elektronicznych, w których mają zastosowanie obiekty, o których mowa w ust. 1, stosują strukturę danych cech informacyjnych tych obiektów zgodną ze strukturą publikowaną przez ministra właściwego do spraw informatyzacji w postaci schematów XML w repozytorium rekomendacji interoperacyjności.

5. Struktura, o której mowa w ust. 4, zawiera w szczególności nazwy i zakresy danych cech informacyjnych obiektów.

6. W przypadkach uzasadnionych specyfiką rejestru prowadzonego przez podmiot realizujący zadanie publiczne może być zastosowany podzbiór cech informacyjnych obiektu, z zachowaniem typu i zakresu danej określonej w schemacie lub rejestr może być rozszerzony o dodatkowe cechy informacyjne.

7. Struktury danych dodatkowych cech informacyjnych muszą być zgłoszone do repozytorium rekomendacji interoperacyjności.

§ 9. Minister właściwy do spraw informatyzacji publikuje na ePUAP schemat XML struktury danych cech informacyjnych obiektów, o których mowa w § 8 ust. 1.

§ 10. 1. Systemy teleinformatyczne, używane przez podmioty realizujące zadania publiczne, powinny być projektowane, wdrażane oraz eksploatowane z uwzględnieniem ich funkcjonalności, niezawodności, używalności, wydajności, przenoszalności i pielęgnowalności, przy zastosowaniu uznanych w obrocie profesjonalnym norm, standardów i metodyk.

2. Zarządzanie usługami realizowanymi przez systemy teleinformatyczne, o których mowa w ust. 1, w szczególności polega na zarządzaniu:

1) incydentem – rozumianym jako przywrócenie normalnego działania usługi w możliwie jak najkrótszym czasie, minimalizując zakłócenia w pracy właściciela usługi w taki sposób, aby zapewnić osiągnięcie możliwie najwyższego poziomu dostępności usługi oraz utrzymanie gwarantowanego poziomu usługi;
2) problemem – rozumianym jako znalezienie przyczyny incydentu i sposobu na przywrócenie poprawnego działania usługi poprzez usunięcie przyczyny incydentu. Zarządzanie problemem minimalizuje niekorzystne konsekwencje występowania błędów w Infrastrukturze;
3) wersją – rozumianym jako planowanie i nadzorowanie pomyślnych wdrożeń nowych wersji oprogramowania oraz zmian wersji oprogramowania jak również związanego z tym sprzętu, dokumentacji i usług;
4) dostępnością usług – rozumianym jako podejmowanie działań zapewniających, że usługa jest dostępna co najmniej na poziomie zdefiniowanym w dokumentacji;
5) ciągłością usług – rozumianym jako wsparcie procesu ciągłości realizacji zadań w podmiocie realizującym zadania publiczne poprzez przywrócenie świadczenia usług w wymaganym i uzgodnionym czasie;

6) pojemnością – rozumianym jako działania zapewniające, że zasoby tworzące infrastrukturę informatyczną odpowiadają rosnącym wymaganiom biznesowym w sposób maksymalnie efektywny kosztowo i czasowo. Zarządzanie pojemnością polega w szczególności na prognozowaniu obciążenia systemu i pojemności elementów systemu, monitorowaniu wykorzystania zasobów w szczególności pod względem pojemności, w szczególności przeglądania logów systemowych, i formułowaniu rekomendacji oraz skalowaniu systemu pod kątem rosnących wymagań;
7) konfiguracją – rozumianym jako działania służące wprowadzeniu logicznego modelu Infrastruktury poprzez identyfikowanie, kontrolę, utrzymanie i weryfikację wersji wszystkich elementów konfiguracji infrastruktury;
8) zmianą – rozumianym jako działania zapewniające, że dla wszystkich zmian zostały przyjęte i są stosowane standardowe metody, procesy i procedury w celu zapewnienia maksymalnej skuteczności i efektywności wprowadzania zmian. Zarządzanie Zmianą zapewnia biznesową równowagę pomiędzy potrzebą zmiany i ryzykiem negatywnego wpływu zmiany na infrastrukturę i usługi;
9) poziomem usług – rozumianym jako utrzymanie jakości usług zdefiniowanych w umowie przez stały cykl uzgadniania, monitorowania, raportowania i przeglądu ich parametrów oraz przez inicjowanie działań w celu likwidacji nieakceptowanego poziomu jakości świadczonych usług;
10) bezpieczeństwem – rozumianym jako działania zgodnie z zasadami gwarantującymi taką eksploatację infrastruktury informatycznej, aby zapewnić bezpieczeństwo informacji rozumiane jako poufność, integralność i dostępność, przy uwzględnieniu autentyczności, rozliczalności, niezaprzeczalności i niezawodności.

3. Wymagania określone w ust. 1 i 2 uznaje się za spełnione jeśli projektowanie, wdrażanie, eksploatowanie, monitorowanie, przeglądanie, utrzymanie i udoskonalanie systemu teleinformatycznego odbywają się z uwzględnieniem Polskich Norm: PN-ISO/IEC 20000-1:2007 „Technika informatyczna – Zarządzanie usługami – Część 1: Specyfikacja", PN-ISO/IEC 20000-2:2007 „Technika informatyczna – Zarządzanie usługami – Część 2: Reguły postępowania" wraz z normami uzupełniającymi lub norm je zastępujących.

§ 11. 1. Systemy teleinformatyczne używane przez podmioty realizujące zadania publiczne wyposaża się w składniki sprzętowe lub oprogramowanie umożliwiające wymianę danych z innymi systemami teleinformatycznymi za pomocą protokołów komunikacyjnych i szyfrujących określonych przez normy, standardy lub rekomendacje ustanowione przez krajową jednostkę normalizacyjną lub jednostkę normalizacyjną Unii Europejskiej.

2. W przypadku, gdy w danej sprawie brak jest norm lub standardów, o których mowa w ust. 1, stosuje się standardy uznane na poziomie międzynarodowym, w szczególności opracowane przez:
1) Internet Engineering Task Force (IETF) i publikowane w postaci Request For Comments (RFC),
2) World Wide Web Consortium (W3C) i publikowane w postaci W3C Recommendation (REC)

- adekwatnie do potrzeb wynikających z realizowanych zadań oraz aktualnego stanu technologii informatycznych,

3. Informację o dostępności opisów standardów, o których mowa w ust. 2, minister właściwy do spraw informatyzacji publikuje w Biuletynie Informacji Publicznej.

4. Kodowanie znaków odbywa się według standardu Unicode UTF-8 określonego przez normę ISO/IEC 10646:2003 „Information technology – Universal Multiple-Octet Coded Character Set" wraz z normami uzupełniającymi lub normą ją zastępującą.

§ 12. 1. Jeżeli dla pisma w formie dokumentu elektronicznego służącego do procedowania danej sprawy nie ustalono wzoru dokumentu elektronicznego lub nie ustanowiono rekomendacji interoperacyjności, systemy teleinformatyczne używane przez podmioty realizujące zadania publiczne powinny umożliwiać przyjmowanie dokumentów w postaci elektronicznej w formatach plików, dla których dostępne jest nieodpłatne oprogramowanie służące do ich odczytania.

2. Systemy teleinformatyczne podmiotów realizujących zadania publiczne powinny udostępniać zasoby informacyjne co najmniej w jednym z formatów plików określonych w załączniku nr 2 do rozporządzenia.

§ 13. 1. Projektując system teleinformatyczny podmiotu realizującego zadania publiczne należy zapewnić realizację przez ten system wymagań Web Content Accessibility Guidelines (WCAG 2.0) na poziomie AA.

2. Minister właściwy do spraw informatyzacji publikuje w Biuletynie Informacji Publicznych listę wymagań, o których mowa w ust. 1.

§ 14. 1. Podmiot realizujący zadania publiczne opracowuje ustanawia, wdraża i eksploatuje, monitoruje i przegląda oraz utrzymuje i doskonali system zarządzania bezpieczeństwem informacji zapewniający poufność, dostępność i integralność informacji, w tym przetwarzanych w systemach teleinformatycznych, z uwzględnieniem takich atrybutów jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność.

2. W szczególności bezpieczeństwo informacji, w systemach teleinformatycznych, uzyskuje się przez:

1) zapewnienie, że kierownictwo podmiotu wspiera i kieruje bezpieczeństwem informacji zgodnie z wymaganiami określonymi przez zadania podmiotu, właściwymi przepisami prawa oraz regulacjami wewnętrznymi;
2) efektywne zarządzanie bezpieczeństwem informacji w podmiocie;
3) utrzymywanie bezpieczeństwa informacji przetwarzanych w podmiocie oraz środków przetwarzania tej informacji, za pomocą których przetwarzają, komunikują się, którymi zarządzają bądź do których mają dostęp osoby lub podmioty zewnętrzne;
4) osiągniecie i utrzymywanie odpowiedniego poziomu ochrony zasobów podmiotu wynikającego z analizy ryzyka;
5) zapewnienie, że informacje uzyskują ochronę na odpowiednim poziomie;
6) zapewnienie, że wszystkie osoby zaangażowane w proces przetwarzania informacji rozumieją swoje obowiązki i są odpowiednio przygotowane do pełnienia wyznaczonych im ról;
7) zredukowanie ryzyka kradzieży lub niewłaściwego korzystania z urządzeń;
8) zapewnienie, że pracownicy, wykonawcy oraz użytkownicy reprezentujący stronę trzecią są świadomi zagrożeń i skutków wynikających z tych zagrożeń dla bezpieczeństwa informacji, swoich

obowiązków i odpowiedzialności prawnej oraz są wyposażeni w niezbędne narzędzia wspomagające politykę bezpieczeństwa podmiotu podczas swej normalnej pracy oraz minimalizujące ryzyko błędów ludzkich;

9) zapewnienie, że pracownicy, wykonawcy i użytkownicy reprezentujący stronę trzecią odchodzą z podmiotu, zaprzestają wykonywać zadania lub zmieniają stanowisko w sposób zorganizowany;
10) zapewnienie w siedzibie podmiotu ochrony przetwarzanych informacji przed nieautoryzowanym dostępem fizycznym, uszkodzeniami lub zakłóceniami;
11) zapobieganie utracie, uszkodzeniu, kradzieży lub naruszeniu zasobów oraz przerwaniu działalności podmiotu;
12) zapewnienie prawidłowej i bezpiecznej eksploatacji środków przetwarzania informacji;
13) wdrożenie i utrzymanie odpowiedniego poziomu bezpieczeństwa informacji i dostaw usług w umowach serwisowych zawartych ze stronami trzecimi;
14) minimalizowanie ryzyka awarii systemów;
15) zapewnienie integralności i dostępności informacji oraz środków przetwarzania informacji;
16) zapewnienie ochrony informacji w sieciach oraz ochrony infrastruktury wspomagającej;
17) zapobieganie nieautoryzowanemu ujawnieniu, modyfikacji, usunięciu lub zniszczeniu informacji;
18) utrzymanie bezpieczeństwa informacji i oprogramowania wymienianego wewnątrz podmiotu oraz z każdym podmiotem zewnętrznym;
19) wykrywanie nieautoryzowanych działań związanych z przetwarzaniem informacji;
20) monitorowanie dostępu do informacji;
21) zapobieganie nieautoryzowanemu dostępowi użytkowników oraz naruszeniu bezpieczeństwa lub kradzieży informacji i środków przetwarzania informacji;
22) ochronę usług sieciowych przed nieautoryzowanym dostępem;
23) ochronę przed nieuprawnionym dostępem do systemów operacyjnych;
24) ochronę przed nieautoryzowanym dostępem do informacji przechowywanych w aplikacjach;
25) zapewnienie bezpieczeństwa informacji przy przetwarzaniu mobilnym i pracy na odległość;
26) zapewnienie, funkcjonowania procedur bezpieczeństwa jako integralnej częścią systemów teleinformacyjnych;
27) ochronę przed błędami, utratą, nieuprawnioną modyfikacją lub nadużyciem informacji w aplikacjach;
28) ochronę poufności, autentyczności i integralności informacji poprzez stosowanie mechanizmów kryptograficznych;
29) zapewnienie bezpieczeństwa plików systemowych;
30) utrzymywanie bezpieczeństwa informacji oraz oprogramowania aplikacyjnego w procesach rozwojowych;
31) redukcję ryzyk wynikających z wykorzystania opublikowanych podatności technicznych systemów teleinformatycznych;

32) zapewnienie, że zdarzenia związane z bezpieczeństwem informacji oraz podatności związane z systemami teleinformatycznymi, są zgłaszane w sposób umożliwiający szybkie podjecie działań korygujących;
33) zapewnie, że stosowane jest spójne i efektywne podejście do zarządzania incydentami związanymi z bezpieczeństwem informacji;
34) zapewnianie kontroli zgodności systemów teleinformatycznych z normami i politykami bezpieczeństwa podmiotu;
35) zapewnienie audytu wewnętrznego w zakresie bezpieczeństwa informacji.

3. System zarządzania bezpieczeństwem informacji spełnia wymogi, o których mowa w ust. 1 i 2, jeżeli został opracowany na podstawie Polskiej Normy PN ISO/IEC 27001:2007 „Technika informatyczna – Techniki bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji – Wymagania" wraz z normami uzupełniającymi lub normy go zastępującej, a ustanawianie zabezpieczeń, zarządzanie ryzykiem oraz audytowanie odbywa się na podstawie Polskich Norm związanych z tą normą, w tym:

1) PN-ISO/IEC 17799:2007 "Technika informatyczna – Techniki bezpieczeństwa – Praktyczne zasady zarządzania bezpieczeństwem informacji",
2) PN-ISO/IEC 27005:2010 "Technika informatyczna – Techniki bezpieczeństwa – Zarządzanie ryzykiem w bezpieczeństwie informacji",
3) PN-ISO/IEC 27006:2009 "Technika informatyczna – Techniki bezpieczeństwa – Wymagania dla jednostek prowadzących audyt i certyfikację systemów zarządzania bezpieczeństwem informacji",
4) PN-ISO/IEC 24762:2010 "Technika informatyczna – Techniki bezpieczeństwa – Wytyczne dla usług odtwarzania techniki teleinformatycznej po katastrofie".

4. W przypadkach uzasadnionych analizą ryzyka lub przepisem prawa w systemach teleinformatycznych podmiotów realizujących zadania publiczne mogą być ustanowione dodatkowe zabezpieczenia niż te, które wynikają z ust. 1 i 2.

§ 15. 1. Rozliczalność w systemach teleinformatycznych podlega dokumentowaniu w postaci elektronicznych zapisów w dziennikach systemów (logach). W uzasadnionych przypadkach dzienniki systemowe mogą być prowadzone w formie pisemnej.

2. W dziennikach systemów, o których mowa w ust. 1, odnotowuje się działania użytkowników lub procesów polegające na dostępie do:

1) systemu z uprawnieniami administracyjnymi;
2) konfiguracji systemu, w tym konfiguracji zabezpieczeń;
3) przetwarzanych w systemach danych podlegających prawnej ochronie.

3. Ustala się czas retencji informacji w dziennikach systemowych, o których mowa w ust. 2, na 2 lata od chwili powstania zapisu.

4. Jeśli przepis szczegółowy ustala dłuższy czas retencji lub retencję wieczystą zapisy logów po upłynięciu czasu, o którym mowa w ust. 3 podlegają archiwizacji na zewnętrznych nośnikach danych.

5. Czas retencji zapisów zawartych w logach zawierających inne informacje niż te, które zostały wymienione w ust. 2, ustala kierownik podmiotu w zależności od ich charakteru i możliwości technicznych, jednak nie krótszy niż 6 miesięcy.

§ 16. Systemy teleinformatyczne podmiotów realizujących zadania publiczne działające w chwili wejścia w życie niniejszego rozporządzenia należy dostosować do wymagań określonych w § 13, najpóźniej w terminie 2 lat od dnia wejścia w życie niniejszego rozporządzenia.

§ 17. Rozporządzenie wchodzi w życie po upływie 14 dni od dnia ogłoszenia[2)].

PREZES

RADY MINISTRÓW

[2)] Niniejsze rozporządzenie było poprzedzone rozporządzeniami: Rady Ministrów z dnia 11 października 2005 r. w sprawie minimalnych wymagań dla systemów teleinformatycznych (Dz. U. Nr 212, poz. 1766) oraz Rady Ministrów z dnia 11 października 2005 r. w sprawie minimalnych wymagań dla rejestrów publicznych i wymiany informacji w formie elektronicznej (Dz. U. Nr 214, poz. 1781), które utraciły moc z dniem 17 grudnia 2010 r. na podstawie art. 14 ustawy z dnia 12 lutego 2010 r. o zmianie ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne i oraz niektórych innych ustaw (Dz. U. Nr 40, poz. 230).

ZAŁĄCZNIK NR 1

IDENTYFIKATORY OBIEKTÓW WYSTĘPUJĄCYCH W ARCHITEKTURZE REJESTRÓW PUBLICZNYCH

Lp.	Nazwa obiektu		Identyfikator obiektu		Definicja Identyfikatora obiektu		Pełna nazwa rejestru publicznego zawierającego dane referencyjne opisujące obiekt	Akt prawny stanowiący podstawę prawną funkcjonowania rejestru, o którym mowa w kolumnie 6
					Długość pola	Typ i zakres danej		
1	2		3		4	5	6	7
1	Osoba fizyczna posiadająca nadany numer PESEL		Numer PESEL		11	Pole znakowe, znaki z zakresu {0..9}	Powszechny Elektroniczny System Ewidencji Ludności	Ustawa z dnia 10 kwietnia 1974 r. o ewidencji ludności i dowodach osobistych (Dz. U. z 2006 r. nr 139, poz. 993, z późn. zm.)
2	Podmiot		Numer REGON		14	Pole znakowe, znaki z zakresu {0..9}	Rejestr publiczny właściwy dla rodzaju podmiotu	Ustawa właściwa dla rodzaju podmiotu
3	Obiekt przestrzenny	Punkt adresowy	Identyfikator punktu adresowego	Identyfikator zasobu informacji przestrzennej (namespace) *)	do 25	Pole znakowe, znaki z zakresu {A .. Z, a .. z, 0 .. 9, _,.,–}	Ewidencja Miejscowości, Ulic i Adresów	Ustawa z dnia 17 maja 1989 r. Prawo geodezyjne i kartograficzne (Dz. U. z 2010 r. Nr 193, poz. 1287)
				Identyfikator lokalny (localId)	do 40			
				Identyfikator wersji (versionId)	25			
		Działka ewidencyjna	Identyfikator działki ewidencyjnej	Identyfikator zasobu informacji przestrzennej (namespace) *)	do 25	Pole znakowe, znaki z zakresu {A .. Z, a .. z, 0 .. 9, _,.,–}	Ewidencja Gruntów i Budynków	
				Identyfikator lokalny (localId)	do 40			
				Identyfikator wersji (versionId)	25			

*) Identyfikator zasobu informacji przestrzennej składa się z dwóch z części:

a) Część pierwsza – dwuliterowy kod państwa, wg definicji określonych w normie ISO 3166, w tym przypadku (PL).

b) Część druga – oznaczenie zasobu informacji przestrzennej, do którego należą obiekty.

ZAŁĄCZNIK NR 2

FORMATY DANYCH ORAZ STANDARDY ZAPEWNIAJĄCE DOSTĘP DO ZASOBÓW INFORMACJI UDOSTĘPNIANYCH ZA POMOCĄ SYSTEMÓW TELEINFORMATYCZNYCH UŻYWANYCH DO REALIZACJI ZADAŃ PUBLICZNYCH

Lp.	Format danych lub skrócona nazwa standardu	Oryginalna pełna nazwa standardu	Opis standardu	Organizacja określająca normę lub standard	Nazwa normy, standardu lub dokumentu normalizacyjnego albo standaryzacyjnego
1	2	3	4	5	6
A	**W celu udostępniania zasobów informacyjnych przez podmiot realizujący zadania publiczne stosuje się:**				
1.	**Do danych zawierających dokumenty tekstowe , tekstowo-graficzne lub multimedialne stosuje się co najmniej jeden z następujących formatów danych:**				
1.1	.txt		Dokumenty w postaci czystego (niesformatowanego) zbioru znaków zapisanych w standardzie Unicode UTF-8 jako pliki typu .txt	ISO	ISO/IEC 10646
1.2	.rtf	Rich Text Format Specification	Dokumenty w postaci sformatowanego tekstu jako pliki typu .rtf	Microsoft Corp.	
1.3	.pdf	Portable Document Format	Dokumenty tekstowo-graficzne jako pliki typu .pdf	Adobe Systems Inc.	
1.4	.doc		Dokumenty w postaci sformatowanego tekstu jako pliki typu .doc	Microsoft Corp.	
1.5	.docx		Dokumenty w postaci sformatowanego tekstu jako pliki typu .docx	Microsoft Corp.	
1.6	.odt	Open Document Format for Office Application	Otwarty format dokumentów aplikacji biurowych	OASIS	

Lp.	Format danych lub skrócona nazwa standardu	Oryginalna pełna nazwa standardu	Opis standardu	Organizacja określająca normę lub standard	Nazwa normy, standardu lub dokumentu normalizacyjnego albo standaryzacyjnego
1	2	3	4	5	6
1.7	Open XML	Office Open Document	Otwarty standard ISO dokumentów elektronicznych	ISO	ISO/IEC 29500
2.	**Do danych zawierających informację graficzną stosuje się co najmniej jeden z następujących formatów danych:**				
2.1	.jpg (.jpeg)	Digital compression and coding of continuous-tone still images	Pliki typu .jpg (Joint Photographic Experts Group)	ISO	ISO 10918
2.2	.gif	Graphics Interchange Format	Pliki typu .gif	CompuServe Inc.	
2.3	.tif (.tiff)	Tagged Image File Format	Pliki typu .tif	Adobe Systems Inc.	
2.4	.geotiff	Geographic Tagged Image File Format	Pliki typu .geotiff	NASA Jet Propulsion Laboratory	GeoTIFF Revision 1.0
2.5	.png	Portable Network Graphics	Plik typu .png	ISO	ISO/IEC 15948:2003
2.6	.svg	Scalable Vector Graphics	Grafika wektorowa	W3C	
3.	**Do kompresji (zmniejszenia objętości) dokumentów elektronicznych o dużych rozmiarach stosuje się co najmniej jeden z następujących formatów danych:**				
3.1	.zip	ZIP file format	Format kompresji plików	PKWAREInc.	
3.2	.tar	Tape Archiver	Format archiwizacji plików (używane zwykle wraz z.gz)	FSF	

Lp.	Format danych lub skrócona nazwa standardu	Oryginalna pełna nazwa standardu	Opis standardu	Organizacja określająca normę lub standard	Nazwa normy, standardu lub dokumentu normalizacyjnego albo standaryzacyjnego
1	2	3	4	5	6
3.3	.gz (.gzip)	GZIP file format	Format kompresji plików	IETF	RFC 1952
3.4	.rar	RAR file format	Format kompresji plików	RarSoft	
4.	**Do tworzenia i modyfikacji stron WWW stosuje się co najmniej jeden z następujących formatów danych:**				
4.1	.html	Hypertext Markup Language	Standard języka znaczników formatujących strony WWW	W3C	
4.2	.xhtml	Extensible Hypertext Markup Language	Standard języka znaczników formatujących strony WWW	W3C	
4.3	.html	Hypertext Markup Language	Standard języka znaczników formatujących strony WWW wykorzystywany w zakresie prezentacji informacji w komputerach kieszonkowych (PDA)	W3C	
4.4	.css	Cascading Style Sheets	Kaskadowy Arkusz Stylu	W3C	
B.	**Do określenia struktury i wizualizacji dokumentu elektronicznego stosuje się następujące formaty danych:**				
1.	**Do definiowania układu informacji polegającego na określeniu elementów informacyjnych oraz powiązań między nimi stosuje się następujące formaty danych:**				
1.1	.xml	Extensible Markup Language	Standard uniwersalnego formatu tekstowego służącego do zapisu danych w formie elektronicznej	W3C	
1.2	.xsd	Extensible Markup Language	Standard opisu definicji struktury dokumentów	W3C	

Lp.	Format danych lub skrócona nazwa standardu	Oryginalna pełna nazwa standardu	Opis standardu	Organizacja określająca normę lub standard	Nazwa normy, standardu lub dokumentu normalizacyjnego albo standaryzacyjnego
1	2	3	4	5	6
			zapisanych w formacie XML		
1.3	.gml	Geography Markup Language	Język Znaczników Geograficznych	OGC	
2.	**Do przetwarzania dokumentów zapisanych w formacie XML stosuje się co najmniej jeden z następujących formatów danych:**				
2.1	.xsl	Extensible Stylesheet Language	Język formatowania danych XML	W3C	
2.2	.xslt	Extensible Stylesheet Language Transformation	Język formatowania danych XML	W3C	
3.	**Do elektronicznego podpisywania i szyfrowania dokumentów elektronicznych stosuje się:**				
1.2	XMLsig	XML-Signature Syntax and Processing	Podpis elektroniczny dokumentów w formacie XML	W3C	
1.3	XAdES	XML Advanced Electronic Signatures	Podpis elektroniczny dokumentów w formacie XML	ETSI	ETSI TS 101 903
1.4	PAdES	PDF Advanced Electronic Signatures	Podpis elektroniczny dokumentów w formacie XML	ETSI	ETSI TS 102 778
	XMLenc	XML Encryption Syntax and Processing	Szyfrowanie dokumentów elektronicznych w formacie XML	W3C	

Objaśnienia skrótów nazw organizacji z kol. 5:

FSF -	Free Software Foundation
IETF -	Internet Engineering Task Force
ISO -	International Standardization Organization
OASIS -	Organization for the Advancement of Structured Information Standards
OGC -	Open Geospatial Consortium Inc.
OMA -	Open Mobile Alliance
W3C -	World Wide Web Consortium
ETSI -	European Telecommunications Standards Institute

Uzasadnienie

Projektowane rozporządzenie wykonuje upoważnienie ustawowe zawarte w art. 18 znowelizowanej ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2005 r. Nr 64, poz. 565, z późn. zm.), zwanej dalej w skrócie ustawą o informatyzacji. W przepisie delegującym występują trzy punkty wskazujące na potrzebę uregulowań prawnych w następujących sprawach:

- minimalnych wymagań dla systemów teleinformatycznych,
- minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej,
- Krajowych Ram Interoperacyjności.

W odniesieniu do minimalnych wymagań dla systemów teleinformatycznych i Krajowych Ram Interoperacyjności dyspozycja delegacji nakazuje uwzględnienie mających zastosowanie Polskich Norm.

Delegacja art. 18 występowała w podobnym brzmieniu przed nowelizacją ustawy o informatyzacji obejmowała jednak tylko dwa pierwsze z wymienionych powyżej punktów, bez Krajowych Ram Interoperacyjności. Skutkowało to tym, że możliwe było wydanie dwóch odrębnych rozporządzeń. Wprowadzenie pojęcia Krajowych Ram Interoperacyjności w zasadniczy sposób zmieniło sytuację. Samo pojęcie ram interoperacyjności wywodzi się z dokumentu powstałego w wyniku projektów IDABC oraz ISA realizowanych na rzecz Komisji Europejskiej w postaci Europejskich Ram Interoperacyjności wersja 2.0. (EIF 2.0). Dokument EIF 2.0 nie stanowi co prawda obowiązującej normy prawnej, należy go jednak traktować jako wytyczną do opracowania Krajowych Ram Interoperacyjności. Pojęcie interoperacyjności występujące w słowniku ustawy o informatyzacji zostało zaczerpnięte z dokumentu EIF. Zgodnie z definicją ustawową interoperacyjności uregulowania normatywne zawarte w przepisach wykonawczych powinny obejmować zagadnienia interoperacyjności semantycznej, organizacyjnej oraz technologicznej. Biorąc pod uwagę, że minimalne wymagania dla systemów teleinformatycznych dotyczą interoperacyjności na poziomie technologicznym, a minimalne wymagania dla rejestrów publicznych i wymiany informacji w postaci elektronicznej dotyczą interoperacyjności semantycznej, a ponadto, że dla każdego z tych obszarów powinny być ustalone wymogi organizacyjne, które są jedną z warstw interoperacyjności wymienianych w EIF 2.0, zasadnym się wydaje wydanie jednego aktu normatywnego w postaci rozporządzenia w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w formie elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych.

Zgodnie z definicją interoperacyjność, to zdolność różnych podmiotów oraz używanych przez nie systemów teleinformatycznych i rejestrów publicznych do współdziałania na rzecz osiągnięcia wzajemnie korzystnych i uzgodnionych celów, z uwzględnieniem współdzielenia informacji i wiedzy przez wspierane przez nie procesy biznesowe realizowane za pomocą wymiany danych za pośrednictwem wykorzystywanych przez te podmioty systemów teleinformatycznych. Z przywołanej definicji wynika, że oddziaływanie prawne powinno dotyczyć zarówno systemów teleinformatycznych wykorzystywanych do realizacji zadań publicznych, jak i spraw organizacyjnych współdziałających podmiotów. W odniesieniu do zagadnień związanych z interoperacyjnością technologiczną oraz organizacyjną delegacja ustawowa nakazuje uwzględnienie norm stanowionych przez Polski Komitet Normalizacji. W obszarze technologii informatycznych obejmujących w pierwszym rzędzie globalną sieć wymiany informacji jaką jest Internet nie ma krajowych norm. Oznacza to, że

w celu zapewnienia współpracy pomiędzy podmiotami realizującymi zadania publiczne z wykorzystaniem tej sieci, w tym współpracy transgranicznej, niezbędne jest korzystanie ze standardów międzynarodowych, w tym przypadku standardów de facto opracowywanych przez Internet Engineering Task Force (IETF).

Podobnie przedstawia się sprawa języka opisu struktur danych wymienianych pomiędzy podmiotami realizującymi zadania publiczne, gdzie zastosowanie mają standardy de facto określane przez World Wide Web Consortium (W3C), powszechnie przyjęte w tym zakresie i sankcjonowane również przez polskie akty normatywne rangi rozporządzenia.

Zgodnie z pojęciem językowym ramy interoperacyjności w kontekście niniejszego rozporządzenia oznaczają zakres lub zasięg oddziaływania przepisów prawa na zagadnienia związane z wymianą informacji przez podmioty realizujące zadania publiczne ze wszystkimi interesariuszami tej wymiany. Ramy interoperacyjności będą określać zarówno sztywne wymogi w postaci wymagań minimalnych, ale też rekomendacje mające za zadanie zapewnienie interoperacyjności w przypadkach fakultatywnych ponad wymagania minimalne. Rekomendacje są dynamiczną częścią Krajowych Ram Interoperacyjności. Ich stosowanie przez podmioty realizujące zadania publiczne powinno być obligatoryjne w obszarze interfejsów łączących systemy informatyczne różnych podmiotów. Wewnątrz systemu rekomendacje takie nie muszą obowiązywać, jednak racjonalne wydaje się stosowanie rozwiązań proponowanych przez rekomendacje i w tym obszarze. Z uwagi na to, że delegacja ustawowa nie sytuuje żadnego organu koordynującego osiąganiem interoperacyjności, jedynym rozwiązaniem pozostaje przypisanie funkcji koordynacyjnych w tym zakresie ministrowi właściwemu do spraw informatyzacji. Takie podejście wynika z przepisu art. 12a ustawy z dnia 4 września 1997 r. o działach administracji rządowej.

Przy tworzeniu systemu zarządzania interoperacyjnością minister powinien kierować się zasadą jawności prac nad ustanawianiem rekomendacji interoperacyjności, a same rekomendacje nie mogą naruszać swobody gospodarczej na rynku usług i dostaw informatycznych, zapewniając równy dostęp do tego rynku wszystkim jego uczestnikom z preferowaniem standardów otwartych.

Architekturę systemu teleinformatycznego należy rozumieć jako proces rozumowania, realizowany podczas opisywania reguł dla całości lub podzbioru zakresu struktury tego systemu, uwzględniający uwarunkowania funkcjonalne, konstrukcyjne, ekonomiczne i inne - istotne dla konkretnego systemu. Strukturę systemu informatycznego opisaną w wyniku jego projektowania architektonicznego nazywa się modelem architektonicznym systemu teleinformatycznego lub modelem architektury systemu.

Ustalając zasady interoperacyjności na poziomie semantycznym należy zdefiniować podstawowe typy obiektów w sferze wymiany informacji pomiędzy podmiotami realizującymi zadania publiczne. Dla każdego z tych obiektów należy wyznaczyć jednoznaczny identyfikator w ramach danego typu oraz określić rejestr publiczny zawierający dane referencyjne. Za rejestr zawierający dane referencyjne należy uznać taki rejestr, w którym dane te są pierwotnie gromadzone. W rozporządzeniu ustalono trzy podstawowe typy obiektów:

- osoba fizyczna, posiadająca nadany numer PESEL;
- osoba prawna, jednostka organizacyjna nie posiadająca osobowości prawnej lub organ władzy publicznej, zwane podmiotem,
- obiekt przestrzenny.

Jako identyfikator osoby fizycznej wskazano numer PESEL, a rejestrem zawierającym dane referencyjne jest rejestr PESEL. W przypadku gdy podmiot publiczny prowadzi rejestr obejmujący osoby fizyczne nieposiadające nadanego numeru PESEL identyfikacja takiej osoby odbywa się według cechy informacyjnej właściwej dla danego rejestru.

W przypadku podmiotu dane referencyjne znajdują się w różnych rejestrach lub dla niektórych podmiotów takich rejestrów nie ma (np. wspólnoty mieszkaniowe). W przypadku podmiotów jednolitym identyfikatorem jest numer REGON. Z numeru REGON można wnioskować o tym gdzie znajduje się rejestr zawierający dane referencyjne.

W odniesieniu do obiektu przestrzennego za jednolite identyfikatory należy uznać identyfikator punktu adresowego i identyfikator działki ewidencyjnej zawarte w rejestrach prowadzonych na podstawie prawa geodezyjnego i kartograficznego. Takie podejście wynika z wdrożenia przepisów Rozporządzenia Komisji (UE) nr 1089/2010 z dnia 23 listopada 2010 r. w sprawie wykonania dyrektywy 2007/2/WE Parlamentu Europejskiego i Rady w zakresie interoperacyjności zbiorów i usług danych przestrzennych. Ponad to w odniesieniu do obiektów przestrzennych w zakresie interoperacyjności mają bezpośrednie zastosowanie przepisy powyższego rozporządzenia KE.

Cechy informacyjne obiektów zawarte będą w rekomendacjach interoperacyjności umieszczonych w repozytorium rekomendacji interoperacyjności.

Podstawowym narzędziem służącym uzyskaniu interoperacyjności są rekomendacje interoperacyjności. Należy zdawać sobie sprawę, że część tych rekomendacji pozostanie poza wpływem polskiej legislacji, jednak ich przyjęcie jest nieuniknione z uwagi na ponadnarodowy charakter takich bytów jak choćby Internet. Zatem standardy i normy dotyczące takich bytów ustalane przez organizacje, których kompetencje wynikają nie z normy prawnej, a z powszechnie i nieformalnie przyjętej zgody nie mogą zostać pominięte. Jednocześnie już dość dawno w dziedzinie produkcji i świadczenia usług zauważono, że efekt synergii działań różnych podmiotów uczestniczących w danym rynku, mimo występującej konkurencyjności, możliwy jest do uzyskania przy wspólnej zgodzie zainteresowanych stron co do przyjmowanych standardów. Podobnie w przypadku interoperacyjności efekt synergii działań podmiotów realizujących zadania publiczne możliwy jest do uzyskania, gdy rekomendacje interoperacyjności zostaną wypracowane nie w sposób nakazowy, a w drodze szerokiego konsensusu. Ważne jest jednak aby stworzone zostały instytucjonalne ramy dla takich uzgodnień oraz aby uzgodnienia były łatwo dostępne. Temu celowi służy umocowanie ministra właściwego do spraw informatyzacji do zarządzania ustalaniem rekomendacji interoperacyjności i publikowania tychże uzgodnień. Możliwość takiego umocowania nie wynika co prawda explicite z delegacji art. 18 ustawy, niemniej implikowana jest ona zadaniami jakie posiada minister właściwy do spraw informatyzacji na podstawie art. 12a pkt 4 ustawy z dnia 4 września 1997 r. o działach administracji rządowej.

Biorąc pod uwagę przepisy ustawy z dnia 12 września 2002 r. o normalizacji może okazać się niezbędne opublikowanie przez Polski Komitet Normalizacyjny niektórych norm i standardów, o których mowa w rozporządzeniu, w polskiej wersji językowej.

Opracowując standardy wymiany informacji w postaci elektronicznej pomiędzy klientami podmiotów realizujących zadania publiczne należy oddzielnie rozpatrywać kierunki komunikacji. W przypadku klientów powinni mieć oni możliwość przesyłania do podmiotów publicznych plików danych, innych niż te, które

określone są we wzorach pism w postaci dokumentów elektronicznych zamieszczonych w centralnym repozytorium, w formatach, które umożliwiają zapoznanie się z treścią takiego pliku z wykorzystaniem nieodpłatnego oprogramowania. Instalacja takiego oprogramowania w podmiocie publicznym, szczególnie w aspekcie spełnienia przez to oprogramowanie warunków bezpieczeństwa, powinna być przedmiotem procedur systemu zarządzania bezpieczeństwem informacji. Liczące się na rynku oprogramowanie służące do wytwarzania plików określonego typu posiada nieodpłatne oprogramowanie umożliwiające odczyt takiego pliku. Umożliwione zatem będzie dostarczanie do podmiotu realizującego zadanie publiczne danych w formatach tworzonych przez specjalistyczne oprogramowanie w sytuacjach gdy po stronie podmiotu publicznego wymagane będzie jedynie zapoznanie się z treścią pliku. Klasycznym przykładem może tu być techniczna dokumentacja budowlana niezbędna do uzyskania pozwolenia na budowę, wytwarzana z wykorzystaniem kosztownego oprogramowania klasy CAD, w sytuacji gdy po stronie organu wydającego decyzję wystarczająca jest operacja odczytu.

Odmiennie wygląda sytuacja, gdy to podmiot publiczny ma udostępniać informacje. Przyjęte do tej wymiany formaty powinny z jednej strony racjonalizować koszt wytworzenia takiej informacji w podmiocie publicznym, a z drugiej zapewniać swobodny do niej dostęp klientów tych podmiotów. Dopuszczalne formaty zostały wymienione enumeratywnie w załączniku nr 2 do rozporządzenia.

Bardzo istotną w zakresie wymagań pozafunkcjonalnych dla systemów teleinformatycznych jest sfera zarządzania bezpieczeństwem informacji. Zarządzanie bezpieczeństwem ma na celu zapewnienie informacji przetwarzanej w systemach podmiotów publicznych zachowania jej dostępności, integralności i poufności z uwzględnieniem takich atrybutów jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność. Dobrą praktyką w zakresie legislacji w tym zakresie jest wskazywanie w aktach normatywnych uznanych na poziomie międzynarodowym norm i standardów. Przykładem takiego podejścia może być Rozporządzenie Komisji (WE) NR 885/2006 (ze zm.) z dnia 21 czerwca 2006 r. ustanawiające szczegółowe zasady stosowania rozporządzenia Rady (WE) nr 1290/2005 w zakresie akredytacji agencji płatniczych i innych jednostek, jak również rozliczenia rachunków EFGR i EFRROW. Załącznik I do rozporządzenia 885/2006 wskazuje na mające zastosowanie normy, w tym normę ISO/IEC 27002. Innym przykładem odwołania do norm może być rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 7 września 2010 r. w sprawie wymagań, jakim powinna odpowiadać ochrona wartości pieniężnych przechowywanych i transportowanych przez przedsiębiorców i inne jednostki organizacyjne, w którym występują odwołania do licznych Polskich Norm. Zatem przywołanie Polskich Norm z zakresu bezpieczeństwa informacji jest zasadne, tym bardziej, że delegacja ustawowa wskazuje na konieczność uwzględnienia w rozporządzeniu Polskich Norm i innych dokumentów normalizacyjnych. Mając to na uwadze jako wiodące w zakresie bezpieczeństwa wskazano Polskie Normy PN ISO/IEC 27001:2007 „Technika informatyczna – Techniki bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji – Wymagania". Z norm związanych z wcześniej wymienionych należy uznać za wskazaną normę PN ISO/IEC 17799:2007 „Technika informatyczna – Techniki bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji – Praktyczne zasady zarządzania bezpieczeństwem informacji" (de facto ISO/IEC 27002). Norma ta wskazuje obszary zabezpieczeń oraz podaje wskazówki metodyczne co do implementacji zabezpieczeń. Jednym z istotnych celów zabezpieczeń ustanawianych w systemach teleinformatycznych, a opisywanych w omawianej normie jest zapewnienie rozliczalności. Służą temu w szczególności zapisy normy PN ISO/IEC 17799 zawarte

rozdziale 10.10 „Monitorowanie” omawiające zabezpieczenia mające na celu wykrywanie nieautoryzowanych działań związanych z przetwarzaniem informacji oraz zapisy rozdziału 11 „Kontrola dostępu” opisujące zabezpieczenia z zakresu dostępu do informacji. W rozporządzeniu w formie przepisów ujęto tylko te zagadnienia, które nie są szczegółowo regulowane w normach, lub normy dopuszczają wielość alternatywnych rozwiązań. Dotyczy to na przykład okresu retencji danych w logach systemów informatycznych gromadzących informacje o aktywności użytkowników i konfiguracjach systemu. Z drugiej strony należy pamiętać, że monitorowanie dostępu do danych wynika z innych przepisów. Na przykład monitorowanie dostępu do danych osobowych wynika z przepisów ustawy o ochronie danych osobowych. Przyjęte w niniejszym rozporządzeniu uregulowania nie uchybiają tym przepisom.

W odniesieniu do eksploatacji systemu teleinformatycznego należy zauważyć, że praktyka wskazuje na wiodąca w tym rolę metodyki ITIL. Metodyka ta stoi u podstaw systemu norm ISO 20000. Zatem w zakresie organizacji i zarządzania w sferze eksploatacji systemu informatycznego powinny być zastosowane metody, o których mówią Polskie Normy PN-ISO/IEC 20000-1:2007 „Technika informatyczna – Zarządzanie usługami – Część 1: Specyfikacja” oraz PN-ISO/IEC 20000-2:2007 „Technika informatyczna – Zarządzanie usługami – Część 2: Reguły postępowania ”, będące krajową implementacją norm międzynarodowych.

Pojęcia z zakresu zarządzania bezpieczeństwem informacji oraz z zakresu zarządzania usługą, umieszczone w § 2 zostały przytoczone w brzmieniu wynikającym z normy ISO/IEC 13335-1:2004

Istotnym obszarem, który reguluje rozporządzenie jest kwestia zwiększenia dostępności do usług eAdministracji dla osób niepełnosprawnych, ze szczególnym uwzględnieniem osób niewidomych i niedowidzących. Konieczność uregulowań prawnych w tym obszarze wynika między innymi ze zobowiązań Polski zawartych w Deklaracji Ministrów państw członkowskich Unii Europejskiej zatwierdzonej jednogłośnie w Rydze w dniu 11 czerwca 2006 r. W związku z tym, że rozwiązania technologiczne w obszarze dostępu osób niewidomych i niedowidzących do treści przekazywanych przez Internet nie są objęte uregulowaniami Polskich Norm zasadne jest wykorzystanie do tego celu „Wytycznych Dotyczących Ułatwień Dostępu Do Zawartości Sieci 2.0" (Web Content Accessibility Guidelines) z 27 kwietnia 2006 roku publikowanych przez powszechnie uznawaną organizację World Wide Web Consortium (W3C). Za minimalny poziom wymagań należy przyjąć poziom AA. Jednocześnie w związku z tym, że dotychczas nie było przepisu określającego wymagania w tym zakresie wprowadza się okres przejściowy, który umożliwi podmiotom publicznym dostosować swoje dotychczasowe serwisy internetowe do tych wymagań.

Ocena skutków regulacji

1. Podmioty, na które oddziałuje projekt rozporządzenia:

Projektowane rozporządzenie ma wpływ na organy administracji publicznej prowadzące systemy teleinformatyczne służące do realizacji zadań publicznych. Rozporządzenie ma ponadto wpływ na sektor informatyki w zakresie dostaw i usług. Wpływ ten ma charakter porządkujący rynek i przeciwdziałający praktykom dyskryminacyjnym oraz wzmacnia przejrzystość podejmowania decyzji w zakresie standardów obowiązujących administrację publiczną podczas formułowania wymagań dla systemów teleinformatycznych służących do realizacji zadań publicznych.

2. Konsultacje społeczne:

W ramach konsultacji społecznych projekt zostanie zamieszczony w Biuletynie Informacji Publicznej na stronie podmiotowej Ministerstwa Spraw Wewnętrznych i Administracji.

Projekt zostanie poddany konsultacjom z następującymi partnerami społecznymi:

- Polskim Towarzystwem Informatycznym (PTI),
- Polską Izbą Informatyki i Telekomunikacji (PIIT),
- Krajową Izbą Gospodarczą Elektroniki i Telekomunikacji (KIGEiT),
- Stowarzyszeniem Instytutu Informatyki Śledczej,
- Związkiem Pracodawców Branży Internetowej Interactive Advertising Bureau Polska,
- Fundacja Wolnego i Otwartego Oprogramowania,
- Fundacja Widzialni.

3. Wpływ regulacji na sektor finansów publicznych, w tym na budżet państwa

Rozporządzenie może mieć wpływ na sektor publiczny z uwagi na konieczność dostosowania systemów teleinformatycznych dla potrzeb osób niepełnosprawnych. Niemniej jednak należy wskazać, iż proces dostosowania został rozłożony w czasie i może być prowadzony w ramach zmian w systemach wynikających z ich cyklu życiowego. Konieczność dostosowania systemów do potrzeb osób niepełnosprawnych wynika również z innych obowiązujących przepisów prawa oraz zobowiązań międzynarodowych.

Rozporządzenie może mieć wpływ na istniejące i znajdujące się w fazie produkcji systemy teleinformatyczne w zakresie zapewnienia bezpieczeństwa informacji w tych systemach.

4. Wpływ regulacji na konkurencyjność gospodarki i przedsiębiorczość, w tym na funkcjonowanie przedsiębiorstw:

Rozporządzenie pozytywnie wpływa na konkurencyjność gospodarki i przedsiębiorczość stwarzając podmiotom gospodarczym równy dostęp do rynku zamówień publicznych w zakresie dostaw i usług informatycznych.

5. Wpływ regulacji na rynek pracy: Nie przewiduje się wpływu projektowanego rozporządzenia na rynek pracy.

6. Wpływ regulacji na sytuację i rozwój regionalny:

Nie przewiduje się wpływu projektowanego rozporządzenia na sytuację i rozwój regionalny.

Rozporządzenie jest zgodne z prawem Unii Europejskiej.