ROZPORZĄDZENIE
RADY MINISTRÓW

z dnia …… 2011 r.

w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych[1)]

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. [2)]) zarządza się, co następuje:

Rozdział I

Przepisy ogólne

§ 1. Rozporządzenie określa:

1) Krajowe Ramy Interoperacyjności;
2) minimalne wymagania dla rejestrów publicznych i wymiany informacji w postaci 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) sposoby zapewnienia dostępu do zasobów informacji podmiotów publicznych dla osób niepełnosprawnych.

§ 2. Użyte w rozporządzeniu określenia oznaczają:

1) architektura systemu teleinformatycznego – opis składników systemu teleinformatycznego, powiązań i relacji pomiędzy tymi składnikami;
2) autentyczność – właściwość polegającą na tym, że pochodzenie lub zawartość danych opisujących obiekt są takie, jak deklarowane;
3) dane referencyjne – dane opisujące cechę informacyjną obiektu pierwotnie wprowadzone do rejestru publicznego w wyniku określonego zdarzenia, z domniemania opatrzone atrybutem autentyczności;

[1)] Niniejsze rozporządzenie zostało notyfikowane Komisji Europejskiej w dniu pod numerem zgodnie z § 4 rozporządzenia Rady Ministrów z dnia 23 grudnia 2002 r. w sprawie sposobu funkcjonowania krajowego systemu notyfikacji norm i aktów prawnych (Dz. U. Nr 239, poz. 2039 oraz z 2004 r. Nr 65, poz. 597), które wdraża dyrektywę 98/34/WE Parlamentu Europejskiego i Rady z dnia 22 czerwca 1998 r. ustanawiającą procedurę udzielania informacji w dziedzinie norm i przepisów technicznych oraz zasad dotyczących usług społeczeństwa informacyjnego (Dz. Urz. WE L 204 z 21.07.1998, str. 37, z późn. zm.; Dz. Urz. UE Polskie wydanie specjalne, rozdz. 13, t. 20, str. 337, z późn. zm.).

[2)] 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, z 2010 r. Nr 40, poz. 230, Nr 167, poz. 1131 i Nr 182, poz. 1228 oraz z 2011 r. Nr 112, poz. 654.

4) dostępność – właściwość określającą, że zasób systemu teleinformatycznego jest możliwy do wykorzystania na żądanie, w założonym czasie, przez podmiot uprawniony do pracy w systemie teleinformatycznym;
5) integralność – właściwość polegającą na tym, że zasób systemu teleinformatycznego nie został zmodyfikowany w sposób nieuprawniony;
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 dla użytkowników zdefiniowano stanowiące odrębną całość funkcje systemu teleinformatycznego (usługi sieciowe) oraz opisano sposób korzystania z tych funkcji, inaczej system zorientowany na usługi (Service Oriented Architecture — SOA);
9) niezaprzeczalność – w rozumieniu przepisów rozporządzenia z dnia 27 kwietnia 2011 r. Ministra Spraw Wewnętrznych i Administracji w sprawie zakresu i warunków korzystania z elektronicznej platformy usług administracji publicznej (Dz. U. Nr 93, poz. 546);
10) obiekt – przedmiot opisu w rejestrze publicznym;
11) obiekt przestrzenny – w rozumieniu przepisów ustawy z dnia 4 marca 2010 r. o infrastrukturze informacji przestrzennej (Dz. U. Nr 76, poz. 489);
12) podatność systemu teleinformatycznego – właściwość systemu teleinformatycznego, która może być wykorzystana przez co najmniej jedno zagrożenie;
13) podmiot – osobę prawną, jednostkę organizacyjną nieposiadającą osobowości prawnej lub organ administracji publicznej;
14) poufność – właściwość zapewniającą, że informacja nie jest udostępniana lub wyjawiana nieupoważnionym osobom fizycznym;
15) polityka bezpieczeństwa informacji – zestaw efektywnych, udokumentowanych zasad i procedur bezpieczeństwa wraz z ich planem wdrożenia i egzekwowania;
16) rekomendacja interoperacyjności – uzgodnienie przyjęte bez stanowiska sprzeciwu pomiędzy interesariuszami regulujące na poziomie organizacyjnym, semantycznym lub technologicznym dowolny aspekt interoperacyjności;
17) repozytorium interoperacyjności – część zasobów ePUAP przeznaczona do udostępniania informacji służących osiąganiu interoperacyjności;
18) rozliczalność – w rozumieniu przepisów rozporządzenia z dnia 21 kwietnia 2011 r. Ministra Spraw Wewnętrznych i Administracji w sprawie szczegółowych warunków organizacyjnych i technicznych, które powinien spełniać system teleinformatyczny służący do identyfikacji użytkowników (Dz. U. Nr 93, poz. 545);
19) usługa sieciowa – właściwość systemu teleinformatycznego polegająca na powtarzalnym wykonywaniu przez ten system z góry określonych funkcji po otrzymaniu, za pomocą sieci teleinformatycznej, danych uporządkowanych w określonej strukturze;

20) ustawa – ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne;
21) wzór dokumentu elektronicznego – wzór, o którym mowa w art. 19b ustawy;
22) zagrożenie systemu teleinformatycznego – potencjalna przyczyna niepożądanego zdarzenia, która może wywołać szkodę w systemie teleinformatycznym.

Rozdział II

Krajowe Ramy Interoperacyjności

§ 3. 1. Krajowe Ramy Interoperacyjności określają:

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 przedsiębiorcom dostępności usług świadczonych przez podmioty realizujące zadania publiczne w postaci elektronicznej,
   b) zwiększenie efektywności usług świadczonych przez administrację publiczną,
   c) zapewnienie obywatelom i przedsiębiorcom zmniejszenia obciążeń związanych z realizacją uprawnień i obowiązków przewidzianych w przepisach odrębnych,
   d) zapewnienie podmiotom publicznym redukcji kosztów funkcjonowania,
   e) zapewnienie racjonalnego gospodarowania funduszami publicznymi,
   f) zapewnienie swobody gospodarczej i równego dostępu do rynku informatycznego w zakresie usług i dostaw podczas udzielania zamówień publicznych dla wszystkich jego uczestników,
   g) efektywną realizację drogą elektroniczną ponadgranicznych usług administracji publicznej;
2) sposoby postępowania podmiotu realizującego zadania publiczne w zakresie przejrzystego wyboru norm, standardów i rekomendacji w zakresie interoperacyjności semantycznej, organizacyjnej oraz technologicznej, z zapewnieniem zasady neutralności technologicznej.

2. Na Krajowe Ramy Interoperacyjności składają się:

1) sposoby osiągania interoperacyjności;
2) architektura systemów teleinformatycznych podmiotów realizujących zadania publiczne;
3) repozytorium interoperacyjności na ePUAP.

§ 4. 1. Interoperacyjność osiąga się przez:

1) ujednolicenie, rozumiane jako zastosowanie kompatybilnych norm, standardów i procedur przez różne podmioty realizujące zadania publiczne, lub
2) wymienność, rozumianą jako możliwość zastąpienia produktu, procesu lub usługi bez jednoczesnego 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, lub

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. Zastosowanie reguł określonych w ust. 1 zależne jest 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 realizujący zadania publiczne sposób osiągnięcia interoperacyjności nie może naruszać zasady neutralności technologicznej.

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

2. Interoperacyjność na poziomie organizacyjnym osiągana jest przez:

1) informowanie przez podmioty realizujące zadania publiczne, w sposób umożliwiający skuteczne zapoznanie się, o sposobie dostępu oraz zakresie użytkowym serwisów dla 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) standaryzację i ujednolicenie procedur z uwzględnieniem konieczności zapewnienia poprawnej współpracy podmiotów realizujących zadania publiczne;
4) publikowanie i uaktualnianie w Biuletynie Informacji Publicznej przez podmiot realizujący zadania publiczne opisów procedur obowiązujących przy załatwianiu spraw z zakresu jego właściwości drogą elektroniczną.

3. Interoperacyjność na poziomie semantycznym osiągana jest przez:

1) stosowanie struktur danych i znaczenia danych zawartych w tych strukturach, określonych w niniejszym rozporządzeniu;
2) stosowanie struktur danych i znaczenia danych zawartych w tych strukturach publikowanych w repozytorium interoperacyjności na podstawie przepisów § 8 ust. 3, § 10 ust. 5, 6, 11 i 12;
3) stosowanie w rejestrach prowadzonych przez podmioty publiczne odwołań do rejestrów zawierających dane referencyjne w zakresie niezbędnym do realizacji zadań.

4. Interoperacyjność na poziomie technologicznym osiągana jest przez:

1) stosowanie minimalnych wymagań dla systemów teleinformatycznych, określonych w rozdziale IV;
2) stosowanie regulacji zawartych w przepisach odrębnych, a w przypadku ich braku uwzględnienia postanowień odpowiednich Polskich Norm, norm międzynarodowych lub standardów uznanych w drodze dobrej praktyki przez organizacje międzynarodowe.

§ 6. W repozytorium interoperacyjności, oprócz struktur danych, o których mowa w § 8 ust. 3 oraz w § 10 ust. 5, 6, 11 i 12, publikuje się także rekomendacje interoperacyjności stanowiące dobre praktyki ułatwiające osiągnięcie interoperacyjności na każdym z poziomów, o których mowa w § 5.

§ 7. 1. Informacje publikowane w repozytorium interoperacyjności oznaczone są w szczególności:

1) nazwą;
2) opisem;
3) wersją;
4) datą i czasem publikacji;
5) statusem obowiązywania;
6) identyfikatorem pozwalającym na identyfikację osoby publikującej.

2. Opublikowana informacja nie może być modyfikowana lub usunięta z repozytorium.

§ 8. 1. Dla systemów teleinformatycznych służących do realizacji zadań publicznych stosuje się rozwiązania oparte na modelu usługowym.

2. Do opisu protokołów i struktur wymiany danych usługi sieciowej wykorzystuje się Web Services Description Language (WSDL).

3. Organ podmiotu udostępniającego usługę sieciową, celem zapewnienia poprawnej współpracy systemów teleinformatycznych przekazuje opis, o którym mowa w ust. 2, do repozytorium interoperacyjności.

4. W przypadkach uzasadnionych specyfiką podmiotu publicznego lub świadczonych przez niego usług dopuszcza się inny model architektury.

§ 9. Minister właściwy do spraw informatyzacji zapewnia:

1) realizację publicznej dyskusji nad rekomendacjami interoperacyjności z zachowaniem zasady neutralności technologicznej oraz zgodności z normami zatwierdzonymi przez krajową jednostkę normalizacyjną lub normami albo standardami rekomendowanymi lub ustalanymi jako obowiązujące przez organy Unii Europejskiej, prowadzonej w sposób, który zapewni każdemu interesariuszowi możliwość realnego wpływu na opracowanie rekomendacji;
2) prowadzenie repozytorium interoperacyjności.

Rozdział III

Minimalne wymagania dla rejestrów publicznych i wymiany informacji w postaci elektronicznej

§ 10. 1. W rejestrach publicznych wyróżnia się w szczególności następujące typy obiektów:

1) osobę fizyczną;
2) podmiot;
3) obiekt przestrzenny.

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

3. Strukturę identyfikatorów typów obiektów, o których mowa w ust. 1 pkt 1 i 2, a także pkt 3 w zakresie dotyczącym punktu adresowego i działki ewidencyjnej, określa załącznik nr 1 rozporządzenia, z zastrzeżeniem ust. 9 i 10.

4. Przepis, o którym mowa ust. 2 w związku z ust. 1 pkt 3 nie wyłącza stosowania przepisów wydanych:

1) w wykonaniu dyrektywy Parlamentu Europejskiego i Rady nr 2007/2/WE z dnia 14 marca 2007 r. ustanawiającej infrastrukturę informacji przestrzennej we Wspólnocie Europejskiej (INSPIRE)

(Dz. Urz. WE L 108 z 25.04.2007, str. 1, z późn. zm.) w zakresie interoperacyjności zbiorów i usług danych przestrzennych;

2) na podstawie art. 19 ust. 1 pkt 6-10 i ust. 1a, art. 24b ust. 4, art. 26 ust. 2 oraz art. 47b ust. 5 ustawy z dnia 17 maja 1989 r. – Prawo geodezyjne i kartograficzne (Dz. U. z 2010 r. Nr 193, poz. 1287).

5. Minister właściwy do spraw informatyzacji publikuje w repozytorium interoperacyjności na ePUAP schemat XML struktury danych cech informacyjnych obiektów, o których mowa w ust. 1.

6. Podmioty realizujące zadania publiczne z wykorzystaniem wymiany informacji za pomocą środków komunikacji elektronicznej 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 interoperacyjności na podstawie wniosków organu prowadzącego rejestr referencyjny właściwy dla danego typu obiektu.

7. W strukturze, o której mowa w ust. 6, należy zawrzeć w szczególności nazwy i zakresy danych cech informacyjnych obiektów.

8. Jeżeli z przepisów prawa wynika, że stosuje się podzbiór cech informacyjnych obiektu, o którym mowa w ust. 1, to zachowuje się typy i zakresy danych określone w schemacie, o którym mowa w ust. 6.

9. Jeśli podmiot publiczny prowadzi rejestr publiczny obejmujący typ obiektu, jakim są osoby fizyczne nieposiadające numeru PESEL, identyfikacja takiej osoby odbywa się według cechy informacyjnej właściwej dla danego rejestru.

10. Jeśli podmiot publiczny prowadzi rejestr publiczny obejmujący typ obiektu, jakim są podmioty nieposiadające nadanego numeru identyfikacyjnego REGON, identyfikacja takiego podmiotu odbywa się według cechy informacyjnej właściwej dla danego rejestru.

11. Struktury danych dodatkowych cech informacyjnych, o których mowa w ust. 9 i 10, podlegają zgłoszeniu do repozytorium interoperacyjności.

12. Organ władzy publicznej, prowadzący rejestr publiczny zawierający obiekty inne niż wymienione w ust. 1, wnioskuje do ministra właściwego do spraw informatyzacji o opublikowanie w repozytorium interoperacyjności, prowadzonym w ramach ePUAP, schematu XML struktur danych cech informacyjnych tych obiektów.

§ 11. 1. Podmiot publiczny prowadzący rejestr publiczny, wydając informacje z tego rejestru w drodze wymiany, jest obowiązany zapewnić rozliczalność takiej operacji.

2. Podmiot otrzymujący informacje z rejestru publicznego w drodze wymiany jest obowiązany do jej ochrony na poziomie nie mniejszym niż ten, który ma zastosowanie w tym rejestrze.

§ 12. Określając funkcjonalność rejestrów publicznych oraz systemów teleinformatycznych, uwzględnia się potrzebę zapewnienia podmiotom uprawnionym realizacji zadań wynikających z odrębnych przepisów.

§ 13. 1. Wymiana danych dokonywana pomiędzy rejestrami publicznymi obejmuje jedynie informacje niezbędne do prawidłowego funkcjonowania tych rejestrów.

2. Wymiana danych, o której mowa w ust. 1, odbywa się przez bezpośrednie odwołanie się do danych referencyjnych przez rejestr inicjujący wymianę.

3. Jeśli wymiana danych w trybie, o którym mowa w ust. 2, jest niemożliwa lub znacznie utrudniona dopuszcza się wymianę danych w innym trybie, w tym przez kopiowanie danych przez rejestr inicjujący wymianę.

§ 14. W trakcie tworzenia lub modernizacji rejestrów publicznych oraz systemów teleinformatycznych uwzględnia się potrzebę zapewnienia bezpłatnego dostępu oraz publikacji w repozytorium interoperacyjności opisów usług, schematów XML oraz innych wzorów.

Rozdział IV

Minimalne wymagania dla systemów teleinformatycznych

§ 15. 1. Systemy teleinformatyczne używane przez podmioty realizujące zadania publiczne projektuje się, wdraża oraz eksploatuje z uwzględnieniem ich funkcjonalności, niezawodności, używalności, wydajności, przenoszalności i pielęgnowalności, przy zastosowaniu norm oraz uznanych w obrocie profesjonalnym standardów i metodyk.

2. Zarządzanie usługami realizowanymi przez systemy teleinformatyczne, o których mowa w ust. 1, ma na celu dostarczanie tych usług na deklarowanym poziomie dostępności i odbywa się w oparciu o udokumentowane procedury.

3. Wymagania określone w ust. 1 i 2 uznaje się za spełnione, jeśli projektowanie, wdrażanie, eksploatowanie, monitorowanie, przeglądanie, utrzymanie i udoskonalanie zarządzania usługą podmiotu realizującego zadanie publiczne odbywają się z uwzględnieniem Polskich Norm: PN-ISO/IEC 20000-1 i PN-ISO/IEC 20000-2.

§ 16. 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 w obowiązujących przepisach, normach, standardach lub rekomendacjach ustanowionych przez krajową jednostkę normalizacyjną lub jednostkę normalizacyjną Unii Europejskiej.

2. W przypadku gdy w danej sprawie brak jest przepisów, 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 bieżącego 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.

§ 17. 1. Kodowanie znaków w dokumentach wysyłanych z systemów teleinformatycznych podmiotów realizujących zadania publiczne lub odbieranych przez takie systemy, także w odniesieniu do informacji wymienianej przez te systemy z innymi systemami na drodze teletransmisji, o ile wymiana ta ma charakter

wymiany znaków, odbywa się według standardu Unicode UTF-8 określonego przez normę ISO/IEC 10646 wraz ze zmianami lub normę ją zastępującą.

2. W uzasadnionych przypadkach dopuszcza się kodowanie znaków według standardu Unicode UTF-16 określonego przez normę, o której mowa w ust. 1.

3. Zastosowanie kodowania, o którym mowa w ust. 2, nie może negatywnie wpływać na współpracę z systemami teleinformatycznymi używającymi kodowania określonego w ust. 1.

§ 18. 1. Systemy teleinformatyczne podmiotów realizujących zadania publiczne udostępniają zasoby informacyjne co najmniej w jednym z formatów danych określonych w załączniku nr 2 do rozporządzenia.

2. Jeżeli z przepisów szczegółowych albo opublikowanych w repozytorium interoperacyjności schematów XML lub innych wzorów nie wynika inaczej, podmioty realizujące zadania publiczne umożliwiają przyjmowanie dokumentów elektronicznych służących do załatwiania spraw należących do zakresu ich działania w formatach danych określonych w załącznikach nr 2 i 3.

§ 19. W systemie teleinformatycznym podmiotu realizującego zadania publiczne służące prezentacji zasobów informacji należy zapewnić spełnienie przez ten system wymagań Web Content Accessibility Guidelines (WCAG 2.0), z uwzględnieniem poziomu AA, określonych w załączniku nr 4 do rozporządzenia.

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

2. Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienie przez kierownictwo podmiotu publicznego warunków umożliwiających realizację i egzekwowanie następujących działań:

1) zapewnienia aktualizacji regulacji wewnętrznych w zakresie dotyczącym zmieniającego się otoczenia;
2) utrzymywania aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji obejmującej ich rodzaj i konfigurację;
3) przeprowadzania okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji oraz podejmowania działań minimalizujących to ryzyko, stosownie do wyników przeprowadzonej analizy;
4) podejmowania działań zapewniających, że osoby zaangażowane w proces przetwarzania informacji posiadają stosowne uprawnienia i uczestniczą w tym procesie w stopniu adekwatnym do realizowanych przez nie zadań oraz obowiązków mających na celu zapewnienie bezpieczeństwa informacji;
5) bezzwłocznej zmiany uprawnień, w przypadku zmiany zadań osób, o których mowa w pkt 4;
6) zapewnienia szkolenia osób zaangażowanych w proces przetwarzania informacji ze szczególnym uwzględnieniem takich zagadnień jak:
    a) zagrożenia bezpieczeństwa informacji,
    b) skutki naruszenia zasad bezpieczeństwa informacji, w tym odpowiedzialność prawna,

c) stosowanie środków zapewniających bezpieczeństwo informacji, w tym urządzenia i oprogramowanie minimalizujące ryzyko błędów ludzkich;

7) zapewnienia ochrony przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami, przez:
   a) monitorowanie dostępu do informacji,
   b) czynności zmierzające do wykrycia nieautoryzowanych działań związanych z przetwarzaniem informacji,
   c) zapewnienie środków uniemożliwiających nieautoryzowany dostęp na poziomie systemów operacyjnych, usług sieciowych i aplikacji;
8) ustanowienia podstawowych zasad gwarantujących bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość;
9) zabezpieczenia informacji w sposób uniemożliwiający nieuprawnionemu jej ujawnienie, modyfikacje, usunięcie lub zniszczenie;
10) zawierania w umowach serwisowych podpisanych ze stronami trzecimi zapisów gwarantujących odpowiedni poziom bezpieczeństwa informacji;
11) ustalenia zasad postępowania z informacjami, zapewniających minimalizację wystąpienia ryzyka kradzieży informacji i środków przetwarzania informacji, w tym urządzeń mobilnych;
12) zapewnienia odpowiedniego poziomu bezpieczeństwa w systemach teleinformatycznych, polegającego w szczególności na:
   a) dbałości o aktualizację oprogramowania,
   b) minimalizowaniu ryzyka utraty informacji w wyniku awarii,
   c) ochronie przed błędami, utratą, nieuprawnioną modyfikacją,
   d) stosowanie mechanizmów kryptograficznych w sposób adekwatny do zagrożeń lub wymogów przepisu prawa,
   e) zapewnieniu bezpieczeństwa plików systemowych,
   f) redukcji ryzyk wynikających z wykorzystania opublikowanych podatności technicznych systemów teleinformatycznych.
   g) niezwłocznym podejmowaniu działań po dostrzeżeniu nieujawnionych podatności systemów teleinformatycznych na możliwość naruszenia bezpieczeństwa,
   h) kontroli zgodności systemów teleinformatycznych z odpowiednimi normami i politykami bezpieczeństwa;
13) bezzwłocznego zgłaszania incydentów naruszenia bezpieczeństwa informacji w określony i z góry ustalony sposób, umożliwiający szybkie podjecie działań korygujących;
14) zapewnienia okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji, nie rzadziej niż raz na rok.

3. Wymagania określone w ust. 1 i 2 uznaje się za spełnione, jeżeli system zarządzania bezpieczeństwem informacji został opracowany na podstawie Polskiej Normy PN-ISO/IEC 27001,

a ustanawianie zabezpieczeń, zarządzanie ryzykiem oraz audytowanie odbywa się na podstawie Polskich Norm związanych z tą normą, w tym:

1) PN-ISO/IEC 17799 – w odniesieniu do ustanawiania zabezpieczeń;
2) PN-ISO/IEC 27005 – w odniesieniu do zarządzania ryzykiem;
3) PN-ISO/IEC 24762 – w odniesieniu do odtwarzania techniki informatycznej po katastrofie w ramach zarządzania ciągłością działania.

4. Niezależnie od zapewnienia działań, o których mowa w ust. 2, w przypadkach uzasadnionych analizą ryzyka w systemach teleinformatycznych podmiotów realizujących zadania publiczne należy ustanowić dodatkowe zabezpieczenia.

§ 21. 1. Rozliczalność w systemach teleinformatycznych podlega wiarygodnemu dokumentowaniu w postaci elektronicznych zapisów w dziennikach systemów (logach).

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

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

3. Poza informacjami wymienionymi w ust. 2 mogą być odnotowywane działania użytkowników lub obiektów systemowych, a także inne zdarzenia związane z eksploatacją systemu w postaci:

1) działań użytkowników nieposiadających uprawnień administracyjnych;
2) zdarzeń systemowych nieposiadających krytycznego znaczenia dla funkcjonowania systemu;
3) zdarzeń i parametrów środowiska, w którym eksploatowany jest system teleinformatyczny

w zakresie wynikającym z analizy ryzyka.

4. Informacje w dziennikach systemów, o których mowa w ust. 2 i 3, przechowywane są od dnia ich zapisu, przez okres wskazany w przepisach odrębnych, a w przypadku braku przepisów odrębnych przez dwa lata.

5. Zapisy dzienników systemów mogą być składowane na zewnętrznych informatycznych nośnikach danych w warunkach zapewniających bezpieczeństwo informacji. W uzasadnionych przypadkach dzienniki systemów mogą być prowadzone na nośniku papierowym.

Rozdział V

Przepisy przejściowe i końcowe

§ 22. Systemy teleinformatyczne podmiotów realizujących zadania publiczne funkcjonujące w dniu wejścia w życie rozporządzenia należy dostosować do wymagań określonych w § 19, nie później niż w terminie 3 lat od dnia wejścia w życie niniejszego rozporządzenia.

§ 23. Systemy teleinformatyczne podmiotów realizujących zadania publiczne funkcjonujące w dniu wejścia w życie rozporządzenia na podstawie dotychczas obowiązujących przepisów należy dostosować do wymagań, o

których mowa w Rozdziale IV rozporządzenia, nie później niż w dniu ich pierwszej istotnej modernizacji przypadającej po wejściu w życie rozporządzenia.

§ 24. Do dnia wejścia w życie przepisów ustanawiających Ewidencję Miejscowości, Ulic i Adresów, rejestrem publicznym wykorzystywanym przy tworzeniu schematu struktury danych punktu adresowego, z wyjątkiem danych, które stanowią współrzędne x, y, jest krajowy rejestr urzędowy podziału terytorialnego kraju, o którym mowa w ustawie z dnia 29 czerwca 1995 r. o statystyce publicznej (Dz. U. Nr 88, poz. 439, z późn. zm.[3)]).

§ 25. Rozporządzenie wchodzi w życie po upływie 14 dni od dnia ogłoszenia.[4)]

PREZES RADY MINISTRÓW

[3)] Zmiany wymienionej ustawy zostały ogłoszone w Dz. U. z 1996 r. Nr 156, poz. 775, z 1997 r. Nr 88, poz. 554 i Nr 121, poz. 769, z 1998 r. Nr 99, poz. 632 i Nr 106, poz. 668, z 2001 r. Nr 100, poz. 1080, z 2003 r. Nr 217, poz. 2125, z 2004 r. Nr 273, poz. 2703, z 2005 r. Nr 163, poz. 1362, z 2006 r. Nr 170, poz. 1217, z 2007 r. Nr 166, poz. 1172, z 2008 r. Nr 227, poz. 1505, z 2009 r. Nr 18, poz. 97, z 2010 r. Nr 47, poz. 278 i Nr 76, poz. 489 oraz z 2011 r. Nr 131, poz. 764, Nr 139, poz. 814, Nr 171, poz. 1016 i Nr 204, poz. 1195.

[4)] 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 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	Wyrażenie regularne
					Długość pola	Typ i zakres danej			
1	2		3		4	5	6	7	8
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.)	\d{11}
2	Podmiot		Numer identyfikacyjny REGON		14	Pole znakowe, znaki z zakresu {0..9}	Rejestr publiczny właściwy dla rodzaju podmiotu. W przypadku podmiotów zarejestrowanych w Krajowym Rejestrze Sądowym rejestrem właściwym jest Krajowy Rejestr Sądowy	Ustawa właściwa dla rodzaju podmiotu	\d{9}|\d{14}
3	Obiekt przestrzenny	Punkt adresowy	Identyfikator punktu adresowego	Przestrzeń nazw (namespace) *)	do 26	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)	PL\.[A-Za-z]{1,6}\.\d{1,6}\.[A-Za-z0-9]{1,8} [A-Za-z0-9]{8}-[A-Za-z0-9]{4}-[A-Za-z0-9]{4}-[A-Za-z0-9]{4}-[A-Za-z0-9]{12} \d{4}-\d\d-\d\dT\d\d:\d\d:\d\d[+\-]\d\d:\d\d
				Identyfikator lokalny (localId)	do 38	Pole znakowe, znaki z zakresu {A .. Z, a .. z, 0 .. 9, _,.,–}			
				Identyfikator wersji (versionId)	do 25	Pole znakowe, znaki z zakresu {T, 0 .. 9, +, -, :}			

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	Wyrażenie regularne
					Długość pola	Typ i zakres danej			
1	2		3		4	5	6	7	8
		Działka ewidencyjna	Identyfikator działki ewidencyjnej	Przestrzeń nazw (namespace) *)	do 26	Pole znakowe, znaki z zakresu {A .. Z, a .. z, 0 .. 9, ,.,}	Ewidencja Gruntów i Budynków		PL\.[A-Za-z]{1,6}\.\d{1,6}\.[A-Za-z0-9]{1,8}
				Identyfikator lokalny (localId)	do 38	Pole znakowe, znaki z zakresu {A .. Z, a .. z, 0 .. 9, _,.,–}			[A-Za-z0-9]{8}-[A-Za-z0-9]{4}-[A-Za-z0-9]{4}-[A-Za-z0-9]{4}-[A-Za-z0-9]{12}
				Identyfikator wersji (versionId)	do 25	Pole znakowe, znaki z zakresu {T, 0 .. 9, +, -, :}			\d{4}-\d\d-\d\dT\d\d:\d\d:\d\d[+\-]\d\d:\d\d

*) Przestrzeń nazw składa się z dwóch z części oddzielonych kropką:

a) część pierwsza – identyfikator zbioru danych przestrzennych nadany zgodnie z przepisami wydanymi na podstawie art. 13 ust. 5 ustawy z dnia 4 marca 2010 r. o infrastrukturze informacji przestrzennej (Dz. U. Nr 76, poz. 489),

b) część druga – literowe oznaczenie zasobu informacji przestrzennej, do której należą obiekty np.: EGiB – dla działki ewidencyjnej, EMUiA – dla punktu adresowego.

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, rozszerzenie nazwy pliku lub skrócona nazwa standardu	Oryginalna pełna nazwa standardu	Opis standardu	Organizacja określająca format, normę lub standard	Oznaczenie lub nazwa normy albo dokumentu zawierającego specyfikację techniczną wskazanego formatu
1	2	3	4	5	6
A	**W celu wymiany zasobów informacyjnych przez podmioty realizujące 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/IEC	ISO/IEC 10646
1.2	.rtf	Rich Text Format Specification	Dokumenty w postaci sformatowanego tekstu jako pliki typu .rtf	Microsoft Corp.	Wewnętrzny standard Microsoft Corp.
1.3	.pdf	Portable Document Format	Dokumenty tekstowo – graficzne jako pliki typu .pdf	ISO/IEC.	ISO/IEC 32000-1
1.4	.xps	XML Paper Specification	Dokumenty tekstowo – graficzne jako pliki typu .xps	Microsoft Corp., Ecma International	ECMA-388
1.5	.odt	Open Document Format for Office Application	Dokumenty w postaci sformatowanego tekstu jako pliki typu .odt	ISO/IEC.	ISO/IEC 26300
1.6	.ods	Open Document Format for Office Application	Dokumenty w postaci sformatowanego arkusza kalkulacyjnego jako pliki typu .ods	ISO/IEC.	ISO/IEC 26300
1.7	.odp	Open Document Format for Office Application	Dokumenty w postaci prezentacji multimedialnych jako pliki typu .odp	ISO/IEC.	ISO/IEC 26300

Lp.	Format danych, rozszerzenie nazwy pliku lub skrócona nazwa standardu	Oryginalna pełna nazwa standardu	Opis standardu	Organizacja określająca format, normę lub standard	Oznaczenie lub nazwa normy albo dokumentu zawierającego specyfikację techniczną wskazanego formatu
1	2	3	4	5	6
1.8	.doc	Microsoft Office Word	Dokumenty w postaci sformatowanego tekstu jako pliki typu .doc	Microsoft Corp.	Wewnętrzny standard Microsoft Corp.
1.9	.xls	Microsoft Office Excel	Dokumenty w postaci sformatowanego arkusza kalkulacyjnego	Microsoft Corp.	Wewnętrzny standard Microsoft Corp.
1.10	.ppt	Microsoft Office PowerPoint	Dokumenty w postaci prezentacji multimedialnych jako pliki typu .ppt	Microsoft Corp	Wewnętrzny standard Microsoft Corp.
1.11	.docx .xlsx .pptx	Office Open XML File Formats	Otwarta specyfikacja techniczna aplikacji biurowych	ISO/IEC	ISO/IEC 29500
1.12	.csv	Comma Separated Values	Wartości rozdzielone przecinkiem	IETF	RFC 4180
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	Plik typu .jpg (Joint Photographic Experts Group)	ISO/IEC	ISO/IEC 10918-1 ISO/IEC 10918-2 ISO/IEC 10918-3 ISO/IEC 10918-4
2.2	.tif (.tiff)	Tagged Image File Format	Plik typu .tif	ISO	ISO 12234-2, ISO 12639
2.3	.geotiff	Geographic Tagged Image File Format	Plik typu .geotiff	NASA Jet Propulsion Laboratory	GeoTIFF Revision 1.0
2.4	.png	Portable Network Graphics	Plik typu .png	ISO/IEC	ISO/IEC 15948

Lp.	Format danych, rozszerzenie nazwy pliku lub skrócona nazwa standardu	Oryginalna pełna nazwa standardu	Opis standardu	Organizacja określająca format, normę lub standard	Oznaczenie lub nazwa normy albo dokumentu zawierającego specyfikację techniczną wskazanego formatu
1	2	3	4	5	6
2.5	.svg	Scalable Vector Graphics (SVG) 1.1 Specification	Plik grafiki wektorowej	W3C	-
3.	**Do danych zawierających informację dźwiękową lub filmową stosuje się odpowiednio co najmniej jeden z następujących formatów danych:**				
3.1	.wav	wave form audio format	plik audio	-	-
3.2	.mp3	MP3 File Format	plik audio	ISO/IEC	ISO/IEC 11172-3 ISOI/IEC 13818-3
3.3	.avi	Audio Video Interleave	niekompresowany plik audio/wideo	IBM Corporation /Microsoft Corporation	
3.4	.mpg .mpeg	MPEG-2 Video Encoding	plik wizualny z dźwiękiem lub bez	ISO/IEC	ISO/IEC 13818
3.5	.mp4 .m4a mpeg4	MPEG-4 Visual Coding	plik wizualny z dźwiękiem lub bez	ISO/IEC	ISO/IEC 14496
3.6	.ogg	Ogg Vorbis Audio Format	plik audio	Xiph.Org Foundation	-
3.7	.ogv	Theora Video Format	plik audiowizualny z dźwiękiem lub bez	Xiph.Org Foundation	-

Lp.	Format danych, rozszerzenie nazwy pliku lub skrócona nazwa standardu	Oryginalna pełna nazwa standardu	Opis standardu	Organizacja określająca format, normę lub standard	Oznaczenie lub nazwa normy albo dokumentu zawierającego specyfikację techniczną wskazanego formatu
1	2	3	4	5	6
4.	**Do kompresji (zmniejszenia objętości) dokumentów elektronicznych stosuje się co najmniej jeden z następujących formatów danych:**				
4.1	.zip	ZIP file format	Format kompresji plików	PKWAREInc.	.ZIP File Format Specification Version: 6.3.2
4.2	.tar	Tape Archiver	Format archiwizacji plików (używane zwykle wraz z.gz)	FSF	-
4.3	.gz (.gzip)	GZIP file format	Format kompresji plików	IETF	RFC 1952
4.4	.7Z	7-Zip file format	Format kompresji plików	Igor Pavlov	-
5.	**Do tworzenia stron WWW stosuje się co najmniej jeden z następujących formatów danych:**				
5.1	.html	Hypertext Markup Language	Standard języka znaczników formatujących strony WWW HTML 4.01	ISO/IEC	ISO/IEC 15445[12]
5.2	.xhtml	Extensible Hypertext Markup Language	Standard języka znaczników formatujących strony WWW	W3C	-
5.3	.html	XHTML Basic 1.1 – Second Edition	Standard języka znaczników formatujących strony WWW wykorzystywany w zakresie prezentacji informacji w komputerach kieszonkowych (PDA) XHTML basic	W3C	-
5.4	.css	Cascading Style Sheets	Kaskadowy Arkusz Stylu	W3C	-

[1] dopuszcza się stosowanie standardu W3C

Lp.	Format danych, rozszerzenie nazwy pliku lub skrócona nazwa standardu	Oryginalna pełna nazwa standardu	Opis standardu	Organizacja określająca format, normę lub standard	Oznaczenie lub nazwa normy albo dokumentu zawierającego specyfikację techniczną wskazanego formatu
1	2	3	4	5	6
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 postaci elektronicznej	W3C	-
1.2	.xsd	Extensible Markup Language	Standard opisu definicji struktury dokumentów zapisanych w formacie XML	W3C	-
1.3	.gml	Geography Markup Language	Język Znaczników Geograficznych	OGC	-
1.4	.rng	REgular LAnguage for XML Next Generation	Język schematów do języka XML	ISO/IEC	ISO/IEC 19757-2
2.	**Do przetwarzania dokumentów zapisanych w formacie XML stosuje się co najmniej jeden z następujących formatów danych:**				
2.1	.xsl	Extensible Stylesheet Language	Rozszerzalny Język Arkuszy Stylów	W3C	-
2.2	.xslt	Extensible Stylesheet Language Transformation	Przekształcenia Rozszerzalnego Języka Arkuszy Stylów	W3C	-

Lp.	Format danych, rozszerzenie nazwy pliku lub skrócona nazwa standardu	Oryginalna pełna nazwa standardu	Opis standardu	Organizacja określająca format, normę lub standard	Oznaczenie lub nazwa normy albo dokumentu zawierającego specyfikację techniczną wskazanego formatu
1	2	3	4	5	6
3.	**Do elektronicznego podpisywania, weryfikacji podpisu i szyfrowania dokumentów elektronicznych stosuje się:**				
3.1	TSL[2]	Trusted Service Status List	Zaufana lista nadzorowanych lub akredytowanych podmiotów świadczących usługi certyfikacyjne	ETSI	ETSI TS 102 231
3.2	XMLsig	XML-Signature Syntax and Processing	Podpis elektroniczny dokumentów w formacie XML	W3C	-
3.3	XAdES[3]	XML Advanced Electronic Signatures	Podpis elektroniczny dokumentów w formacie XML	ETSI	ETSI TS 101 903
3.4	PAdES[3]	PDF Advanced Electronic Signatures	Podpis elektroniczny dokumentów w formacie PDF	ETSI	ETSI TS 102 778
3.5	CAdES[3]	CMS Advanced Electronic Signatures	Podpis elektroniczny dokumentów w formacie CMS	ETSI	ETSI TS 101 733
3.6	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

[2] Wykorzystanie list TSL w systemach administracji publicznej następuje w oparciu o najnowszą wersję standardu ETSI TS 102 231 oraz europejski system list TSL w zgodzie z decyzją Komisji 2009/767/WE z dnia 16 października 2009 r. ustanawiająca środki ułatwiające korzystanie z procedur realizowanych drogą elektroniczną poprzez "pojedyncze punkty kontaktowe" zgodnie z dyrektywą 2006/123/WE Parlamentu Europejskiego i Rady dotyczącą usług na rynku wewnętrznym (Dz. U. UE L 274 z 20.10.2009, str. 36, z późn. zm.).

[3] Stosowane zgodnie z Decyzją Komisji z dnia 25 lutego 2011 r. w sprawie ustalenia minimalnych wymagań dotyczących transgranicznego przetwarzania dokumentów podpisanych elektronicznie przez właściwe organy zgodnie z dyrektywą 2006/123/WE Parlamentu Europejskiego i Rady dotyczącą usług na rynku wewnętrznym (Dz. U. UE L 53 z 25.02.2011, str. 66).

ZAŁĄCZNIK NR 3

FORMATY DANYCH OBSŁUGIWANE PRZEZ PODMIOT REALIZUJĄCY ZADANIE PUBLICZNE W TRYBIE ODCZYTU

Lp.	Rozszerzenie nazwy pliku	Oryginalna pełna nazwa formatu	Opis formatu	Organizacja określająca normę lub standard	Nazwa normy, standardu lub dokumentu normalizacyjnego albo standaryzacyjnego
1	2	3	4	5	6
1.	.dwg	-	plik binarny programu AutoCAD z grafiką wektorową	Autodesk	Wewnętrzny format Autodesk
2.	.dwf	-	skompresowany plik programu AutoCAD	Autodesk	Wewnętrzny format Autodesk
3.	.dxf	-	plik programu AutoCAD kodowany znakami ASCII	Autodesk	Wewnętrzny format Autodesk
4.	.dgn	-	pliki programu MicroStation z grafiką wektorową	Bentley Systems	Wewnętrzny format Bentley Systems
5.	.jp2	Joint Photographic Experts Group 2000	Format graficzny JPEG2000	ISO/IEC	ISO/IEC 15444-1

ZAŁĄCZNIK NR 4

WYMAGANIA *Web Content Accessibility Guidelines* (WCAG 2.0) DLA SYSTEMÓW TELEINFORMATYCZNYCH W ZAKRESIE DOSTĘPNOŚCI DLA OSÓB NIEPEŁNOSPRAWNYCH

W systemie teleinformatycznym podmiotu służącym do realizacji zadania publicznego należy zapewnić spełnienie następujących wymagań:

Lp.	Zasada	Wymaganie	Pozycja w WCGA 2.0	Poziom
1.	Zasada 1 – Postrzeganie	Wymaganie 1.1	1.1.1	A
2.		Wymaganie 1.2	1.2.1	A
3.			1.2.2	
4.			1.2.3	
5.		Wymaganie 1.3	1.3.1	A
6.			1.3.2	
7.			1.3.3	
8.		Wymaganie 1.4	1.4.1	A
9.			1.4.2	
10.			1.4.3	AA
11.			1.4.4	
12.			1.4.5	
13.	Zasada 2 – Funkcjonalność	Wymaganie 2.1	2.1.1	A
14.			2.1.2	
15.		Wymaganie 2.2	2.2.1	A
16.			2.2.2	
17.		Wymaganie 2.3	2.3.1	A
18.		Wymaganie 2.4	2.4.1	A
19.			2.4.2	
20.			2.4.3	
21.			2.4.4	
22.			2.4.5	AA
23.			2.4.6	
24.			2.4.7	
25.	Zasada 3 – Zrozumiałość	Wymaganie 3.1	3.1.1	A
26.			3.1.2	AA
27.		Wymaganie 3.2	3.2.1	A
28.			3.2.2	
29.			3.2.3	AA
30.			3.2.4	
31.		Wymaganie 3.3	3.3.1	A
32.			3.3.2	
33.			3.3.3	AA
34.			3.3.4	
35.	Zasada 4 – Kompatybilność	Wymaganie 4.1	4.1.1	A
36.			4.1.2	

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 został zamieszczony w Biuletynie Informacji Publicznej na stronie podmiotowej Ministerstwa Spraw Wewnętrznych i Administracji.

Projekt został 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,
- Fundacją Wolnego i Otwartego Oprogramowania,
- Fundacją Widzialni.

Do pierwszej wersji projektu uwagi zgłosili przedstawiciele Polskiej Izby Informatyki i Teleinformatyki , Polskie Towarzystwo Informatyczne, Fundacja Widzialni, Fundacja Instytutu Rozwoju Regionalnego, Fundacja Wolnego i Otwartego Oprogramowania, oraz osoba fizyczna Pan Paweł Krawczyk. Podmioty reprezentujące stronę społeczną zgłosiły do pierwszego projektu ogółem 93 uwagi. Wszystkie zgłoszone uwagi, również te uwzględnione, zostały omówione na pierwszej konferencji uzgodnieniowej, która miała miejsce 15 kwietnia 2011 r. Waga rozporządzenia oraz bardzo duże zainteresowanie projektem aktu prawnego oraz złożoność omawianych uwag wymagały przeprowadzenia kolejnej, drugiej konferencji uzgodnieniowej, która odbyła się dnia 5 maja 2011 r. Do treści projektu opracowanej i przesłanej uczestnikom po drugiej konferencji uwagi zgłosili m. in. przedstawiciele Fundacji Wolnego i Otwartego Oprogramowania oraz Polska Izba Informatyki Telekomunikacji. Treść projektu opracowana po rozpatrzeniu niniejszych uwag zmieniana była kilkakrotnie, również w zakresie wcześnie zgłaszanych przez stronę społeczną postulatów. Zmiany te niejednokrotnie prowadziły do zdecydowanej zmiany w treści przepisów, co do których we wcześniejszych terminach przyjęto ustalenia. Dlatego też zmiany w kolejnych wersjach przebiegały bardzo dynamicznie, co wymagało przeprowadzenia również uzgodnień o charakterze bilateralnym jakie na przykład miały miejsce dnia 25 oraz 27 maja 2011.

Mając na uwadze powyższe MSWiA po zasięgnięciu opinii RCL uznało, iż z uwagi na bardzo duże zmiany w treści projektu niezbędnym jest jego ponowne wysłanie do wszystkich podmiotów zainteresowanych

brzmieniem projektu. Do niniejszej wersji projektu rozporządzenia ze strony społecznej uwagi wystosowała Polska Izba Informatyki i Telekomunikacji.

Uwaga pierwsza wskazywała, iż w opinii PIIT należy zawrzeć przepis wskazujący, iż w systemie teleinformatycznym podmiotu realizującego zadania publiczne stosuje się język polski. Jako uzasadnienie swojego stanowiska PIIT wskazuje na art. 4 oraz art. 9 i 10 ustawy z dnia 7 października 1999 r. o języku polskim (Dz. U. 2011 Nr 43, poz. 224). Zapis proponowany przez PIIT jest w opinii MSWiA zbędny gdyż przepis ustawy we wskazanym przez nią zakresie podmiotowym oraz przedmiotowym stosuje się bez potrzeby wskazywania tego faktu w akcie rangi rozporządzenia.

Uwaga druga podkreślała, iż PIIT wyraża pogląd, że z definicji rekomendacji Interoperacyjności zawartej w art. 2 pkt 16 należy wykreślić wyrażenie „bez stanowiska sprzeciwu", wskazując, że taki zapis wprowadza de facto instytucje „liberum veto". Uwaga ta nie została uwzględniona gdyż instytucja rekomendacji w opinii MSWiA powinna prowadzić do wypracowania stanowiska w drodze konsensusu, a więc jednomyślnie. Natomiast brak jednomyślności skutkował będzie brakiem ustalenia rekomendacji, a w konsekwencji będzie prowadził do stosowania standardów nie niższych niż określone niniejszym rozporządzeniem.

W uwadze trzeciej podkreślono, że w § 5 ust 4, który stwierdza, że Interoperacyjność na poziomie technologicznym osiągana jest poprzez stosowanie rozwiązań zawartych w przepisach § 15 – 21 oraz stosowanie regulacji zawartych w przepisach odrębnych, a w przypadku ich braku Polskich Norm, norm międzynarodowych lub standardów uznanych w drodze dobrej praktyki przez organizacje międzynarodowe należy wykreślić wyrazy „w drodze dobrej praktyki". Propozycja ta uzasadniona została stwierdzeniem, iż standardy w każdej organizacji są przyjmowane według określonej procedury. Stanowisko to nie zostało uwzględnione, gdyż co prawda nie sposób odmówić racji argumentowi przytoczonemu przez PIIT, niemniej jednak dobra praktyka bardzo często jest powszechnie uznawanym w takiej organizacji uzupełnieniem przyjętych procedur. Ponadto określenie to nie wpływa negatywnie na treść merytoryczną projektu, natomiast wskazuje porządny kierunek osiągania interoperacyjności .

Przedmiotowy projekt został uzgodniony i zaakceptowany przez Zespół ds. Społeczeństwa Informacyjnego Komisji Wspólnej Rządu i Samorządu Terytorialnego. Zespół ten został w dniu 30 marca 2011 r. upoważniony przez Komisje Wspólną Rządu i Samorządu Terytorialnego do zajęcia w przedmiotowej sprawie wiążącego stanowiska, które zapadło na posiedzeniu w dniu 19 lipca 2011 r.

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.

Wprowadzony w projekcie rozporządzenia § 19 odnosi się przede wszystkim do systemów nowotworzonych oraz modernizowanych po dniu wejścia w życie niniejszego rozporządzenia. Ponadto w

projekcie rozporządzenia uwzględniono przepis przejściowy, który stanowi, że systemy teleinformatyczne funkcjonujące w dniu wejścia w życie rozporządzenia na podstawie dotychczas obowiązujących przepisów, zostaną dostosowane do wymogów o których mowa w Rozdziale IV rozporządzenia nie później niż w dniu ich modernizacji przypadającej po wejściu w życie rozporządzenia. Zapis ten chroni podmioty na które będzie oddziaływał projektowany akt prawny przed generowaniem kosztów innych niż, jak już wskazano powyżej, wynikających z ich cyklu życiowego. Dodatkowo należy podkreślić, że dnia modernizacji systemu nie należy utożsamiać z dniem wprowadzenia zmian kodu wykonywalnego do systemu teleinformatycznego, a należy rozumieć go jako moment podjęcia decyzji o przystąpieniu do prac projektowych mających skutkować modernizacją.

Ponadto adresaci rozporządzenia nie będą zobligowani do podniesienia dodatkowych kosztów związanych z zakupem polskich norm w celu prawidłowej realizacji wymogów niniejszego rozporządzenia, gdyż wymagania te obowiązywały już na podstawie § 3 ust. 2 rozporządzenia Rady Ministrów z dnia 11 października 2005 r. w sprawie minimalnych wymagań dla systemów teleinformatycznych (Dz. U. Nr 212, poz. 1766)

Ewentualne koszty związane ze zmianami w systemach teleinformatycznych podmiotów realizujących zadania publiczne będą pokrywane w ramach środków ujętych w planach finansowych jednostek sektora finansów publicznych, a w przypadku budżetu państwa będą finansowane w ramach limitu wydatków ustalanego we właściwych częściach budżetowych ustawy budżetowej.

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.

Uzasadnienie

Projekt rozporządzenia zgodnie z art. 5 ustawy z dnia 7 lipca 2005 r. *o działalności lobbingowej w procesie stanowienia prawa* (Dz.U. Nr 169, poz. 1414, z późn. zm.) został udostępniony w Biuletynie Informacji Publicznej.

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 wydaje się wydanie jednego aktu normatywnego w formie rozporządzenia w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych. Jednocześnie stosując zasadę przechodzenia od uregulowań ogólnych do szczegółowych należy w rozporządzeniu opisać kolejno: Krajowe Ramy Interoperacyjności, minimalne wymagania dla rejestrów publicznych i wymiany informacji w postaci elektronicznej, 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, często nie ma norm krajowych. 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 mieć zastosowanie przede wszystkim 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 należy 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.

Interoperacyjność można uzyskać na kilka sposobów, w tym poprzez: ujednolicenie, wymienność lub zgodność. Podstawowym sposobem powinno być osiąganie interoperacyjności poprzez zapewnienie wymienności. Należy jednak zauważyć, że nie można wykluczyć pozostałych dwóch sposobów. Należy zaznaczyć, że w przypadku ujednolicenia zastosowanie tego sposobu nie wyklucza stosowania prawa zamówień publicznych i nie znosi obowiązku zapewnienia neutralności technologicznej. Należy ponadto zauważyć, że zastosowany sposób osiągania interoperacyjności nie musi odnosić się do całego systemy teleinformatycznego podmiotu realizującego zadanie publiczne, ale może dotyczyć pewnych jego części składowych.

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,
- 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 lub w przepisie sytuującym rejestr wskazano na inny identyfikator, 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 identyfikacyjny REGON. Z rejestru 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. Ponadto w odniesieniu do obiektów przestrzennych w zakresie interoperacyjności mają bezpośrednie zastosowanie przepisy powyższego rozporządzenia KE.

Cechy informacyjne obiektów zawarte będą w repozytorium interoperacyjności.

Podstawowym narzędziem służącym uzyskaniu interoperacyjności są rekomendacje interoperacyjności. Informacje publikowane w repozytorium interoperacyjności oznaczone są m. in. identyfikatorem pozwalającym na identyfikację osoby publikującej. Celem takiego oznaczenia jest uzyskanie możliwości określenia osoby dokonującej zmian w repozytorium i jest on możliwy do osiągnięcia za pomocą ww. identyfikatora, który jest zwykłym podpisem cyfrowym. Mając na uwadze niniejsze należy wskazać, iż niepotrzebnym byłoby zastępowanie tegoż identyfikatora bezpiecznym podpisem elektronicznym z punktu widzenia celu, dla osiągnięcia którego identyfikator został wprowadzony w przepisach .

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 innych dokumentów normalizacyjnych, o których mowa w rozporządzeniu, w polskiej wersji językowej.

Wskazane w § 10 ust. 1 pkt rozporządzenia podmioty nie mogą być rozumiane jedynie jako podmioty gospodarki narodowej. Rozumienie takie było by zgodne z postrzeganą w systemie REGON osobą fizyczną prowadzącą działalność gospodarczą, osobą prawną oraz jednostką organizacyjną nie mającą osobowości prawnej. Niemniej jednak jest to niedopuszczalne z uwagi na wykluczenie podmiotów nie posiadających numerów REGON z katalogu podmiotów, do który stosował by się niniejszy przepis, co jest sprzeczne z ideą rozporządzenia.

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. Z drugiej jednak strony może pojawić się możliwość przedkładania przez nadawców egzotycznych formatów danych i wskazywania równie egzotycznych programów służących do ich odczytywania. Mogłoby to być w prosty sposób wykorzystywane do prób instalacji w systemach podmiotu

publicznego oprogramowania szkodliwego. W związku z tym, podtrzymując ideę możliwości dostarczania do podmiotu publicznego plików wytworzonych za pomocą specjalistycznego oprogramowania w rozporządzeniu zamieszczono wykaz plików, które muszą być przyjmowane przez podmiot publiczny. Z uwagi na to, że są to wymagania minimalne podmiot publiczny może określić jakie inne typy plików mogą być do tego podmiotu dostarczane przez jego petentów.

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.

Rozporządzenie wskazuje, iż regułą jest sytuacja w której rozliczalność w systemach teleinformatycznych podlega wiarygodnemu dokumentowaniu w postaci elektronicznej zapisów w dziennikach systemów, prowadzonych w tych systemach. Niemniej jednak wprowadza jednocześnie pewne odstępstwa od tej reguły. Pierwsze z nich daje możliwość składowania zapisów dzienników systemów na zewnętrznych informatycznych nośnikach danych, szczególnie w przypadkach gdy zapisy dziennika osiągają znaczne wolumeny. Drugie zaś umożliwia w uzasadnionych przypadkach, wynikających ze specyfiki zapisywanych danych, prowadzenie dzienników systemów na nośniku papierowym.

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.

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. Trzy letni okres przejściowy podyktowany jest tym, że budżet na rok 2012 został już zamknięty i nie jest możliwe ujęcie przedsięwzięć związanych dostosowaniem systemów teleinformatycznych w planach finansowych na ten rok.

W trakcie uzgodnień międzyresortowych strona społeczna zgłosiła uwagę w myśl której przepis § 19 rozporządzenia powinien stanowić, iż „W systemie teleinformatycznym podmiotu realizującego zadania publiczne należy zapewnić spełnienie przez ten system wymagań Web Content Accessibility Guidelines (WCAG 2.0) z uwzględnieniem poziomu AA". Uwag ta nie może zostać uwzględniona, gdyż art. 18 ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne wskazuje w pkt 1 lit. c, iż Rada Ministrów, na wniosek ministra właściwego do spraw informatyzacji, określi w drodze rozporządzenia minimalne wymagania dla systemów teleinformatycznych, mając na uwadze konieczność zapewnienia „dostępu do zasobów informacji osobom niepełnosprawnym". Natomiast propozycja strony społecznej

przewiduje również konieczność zapewnienia możliwości tworzenia tychże zasobów, co wykracza poza treść przytoczonych przepisów.

Rozporządzenie jest zgodne z prawem Unii Europejskiej.

Rozporządzenie podlega notyfikacji.