DZIENNIK USTAW
RZECZYPOSPOLITEJ POLSKIEJ

Warszawa, dnia 22 maja 2024 r.

Poz. 773

ROZPORZĄDZENIE
RADY MINISTRÓW

z dnia 21 maja 2024 r.

w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci 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. z 2024 r. poz. 307) zarządza się, co następuje:

Rozdział 1

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.

§ 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;

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 – brak możliwości zanegowania swego uczestnictwa w całości lub w części wymiany danych przez jeden z podmiotów uczestniczących w tej wymianie;

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. z 2021 r. poz. 214);

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 przeznaczoną do udostępniania informacji służących osiąganiu interoperacyjności;

18) rozliczalność – właściwość systemu pozwalającą przypisać określone działanie w systemie do osoby fizycznej lub procesu oraz umiejscowić je w czasie;

19) usługa sieciowa – właściwość systemu teleinformatycznego polegającą na powtarzalnym wykonywaniu przez ten system z góry określonych funkcji po otrzymaniu, za pomocą sieci teleinformatycznej, danych uporządkowanych w określonej strukturze;

20) ustawa – ustawę 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 – potencjalną przyczynę niepożądanego zdarzenia, która może wywołać szkodę w systemie teleinformatycznym.

Rozdział 2

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 oraz § 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 4;

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, w celu 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 3

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, z zastrzeżeniem ust. 9 i 10, określa załącznik nr 1 do rozporządzenia.

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

1) w wykonaniu dyrektywy 2007/2/WE Parlamentu Europejskiego i Rady z dnia 14 marca 2007 r. ustanawiającej infrastrukturę informacji przestrzennej we Wspólnocie Europejskiej (INSPIRE) (Dz. Urz. UE L 108 z 25.04.2007, str. 1, z późn. zm.[1)]) 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 2023 r. poz. 1752, 1615, 1688 i 1762).

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 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.

[1)] Zmiany wymienionej dyrektywy zostały ogłoszone w Dz. Urz. UE L 73 z 15.03.2008, str. 36 oraz Dz. Urz. UE L 170 z 25.06.2019, str. 115.

Rozdział 4

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 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 do rozporządzenia.

§ 19. 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) stosowaniu 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 podjęcie 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 27002 – w odniesieniu do ustanawiania zabezpieczeń;

2) PN-ISO/IEC 27005 – w odniesieniu do zarządzania ryzykiem.

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.

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

2. W dziennikach systemów 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 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 5

Przepis końcowy

§ 21. Rozporządzenie wchodzi w życie z dniem następującym po dniu ogłoszenia.[2)]

Prezes Rady Ministrów: *D. Tusk*

[2)] Niniejsze rozporządzenie było poprzedzone rozporządzeniem Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. z 2017 r. poz. 2247), które traci moc z dniem wejścia w życie niniejszego rozporządzenia na podstawie art. 26 ustawy z dnia 4 kwietnia 2019 r. o dostępności cyfrowej stron internetowych i aplikacji mobilnych podmiotów publicznych (Dz. U. z 2023 r. poz. 1440).

Załączniki do rozporządzenia Rady Ministrów
z dnia 21 maja 2024 r. (Dz. U. poz. 773)

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 24 września 2010 r. o ewidencji ludności (Dz. U. z 2024 r. poz. 736)	\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 2023 r. poz. 1752, z późn. zm.)	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}
				Identyfikator lokalny (localId)	do 38	Pole znakowe, znaki z zakresu {A .. Z, a .. z, 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
				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
		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 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. z 2021 r. poz. 214),

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 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

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
1.6	.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
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

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.	**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
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	

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
3.4	.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	-
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	-

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
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[1)]
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, opatrywania pieczęcią elektroniczną 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 119 612
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 103 171
3.4	PAdES[3)]	PDF Advanced Electronic Signatures	Podpis elektroniczny dokumentów w formacie PDF	ETSI	ETSI TS 103 172
3.5	CAdES[3)]	CMS Advanced Electronic Signatures	Podpis elektroniczny dokumentów w formacie CMS	ETSI	ETSI TS 103 173
3.6	ASIC[3)]	Associated Signature Containers	Podpis elektroniczny dokumentów wykorzystujący kontener ZIP	ETSI	ETSI TS 103 174
3.7	XMLenc	XML Encryption Syntax and Processing	Szyfrowanie dokumentów elektronicznych w formacie XML	W3C	-

2) Wykorzystanie list TSL w systemach administracji publicznej następuje w oparciu o najnowszą wersję standardu ETSI TS 119 612 oraz europejski system list TSL zgodnie z decyzją wykonawczą Komisji (UE) 2015/1505 z dnia 8 września 2015 r. ustanawiającą specyfikacje techniczne i formaty dotyczące zaufanych list zgodnie z art. 22 ust. 5 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym (Dz. Urz. UE L 235 z 09.09.2015, str. 26 oraz Dz. Urz. UE L 59 z 07.03.2017, str. 41).

3) Stosowane zgodnie z decyzją wykonawczą Komisji (UE) 2015/1506 z dnia 8 września 2015 r. ustanawiającą specyfikacje dotyczące formatów zaawansowanych podpisów elektronicznych oraz zaawansowanych pieczęci elektronicznych, które mają być uznane przez podmioty sektora publicznego, zgodnie z art. 27 ust. 5 i art. 37 ust. 5 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym (Dz. Urz. UE L 235 z 09.09.2015, str. 37).

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

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