II

(Akty o charakterze nieustawodawczym)

ROZPORZĄDZENIA

ROZPORZĄDZENIE WYKONAWCZE KOMISJI (UE) NR 1179/2011

z dnia 17 listopada 2011 r.

ustanawiające specyfikacje techniczne w odniesieniu do systemów zbierania deklaracji *on-line* na mocy rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 211/2011 w sprawie inicjatywy obywatelskiej

KOMISJA EUROPEJSKA,

uwzględniając Traktat o funkcjonowaniu Unii Europejskiej,

uwzględniając rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 211/2011 z dnia 16 lutego 2011 r. w sprawie inicjatywy obywatelskiej [1], w szczególności jego art. 6 ust. 5,

po konsultacji z Europejskim Inspektorem Ochrony Danych

a także mając na uwadze, co następuje:

(1) Rozporządzenie (UE) nr 211/2011 stanowi, że w przypadku zbierania deklaracji poparcia *on-line* system używany do tego celu musi spełniać pewne wymogi bezpieczeństwa i wymogi techniczne oraz musi posiadać certyfikat wydany przez właściwy organ danego państwa członkowskiego.

(2) System zbierania deklaracji *on-line* w rozumieniu rozporządzenia (UE) nr 211/2011 jest systemem informatycznym, obejmującym oprogramowanie, sprzęt, środowisko hostingowe, procesy biznesowe i personel, służącym do gromadzenia deklaracji poparcia *on-line*.

(3) Rozporządzenie (UE) nr 211/2011 określa wymogi, które systemy zbierania deklaracji *on-line* muszą spełniać w celu uzyskania certyfikatu, oraz stanowi, że Komisja powinna przyjąć specyfikacje techniczne w celu wprowadzenia w życie tych wymogów.

(4) Opracowanie „Top 10 2010" stworzone przez organizację OWASP (Open Web Application Security Project) zawiera przegląd zarówno największych zagrożeń dotyczących bezpieczeństwa aplikacji sieciowych, jak i narzędzi do ich eliminowania; w związku z czym specyfikacje techniczne są oparte na wynikach wspomnianego opracowania.

(5) Wdrożenie specyfikacji technicznych przez organizatorów powinno zagwarantować wydanie przez władze państw członkowskich certyfikatów dla systemów zbierania deklaracji *on-line* oraz przyczynić się do wprowadzenia w życie odpowiednich środków technicznych i organizacyjnych wymaganych do wykonania zobowiązań nałożonych dyrektywą 95/46/WE Parlamentu Europejskiego i Rady [2] w sprawie bezpieczeństwa przetwarzania danych, zarówno w czasie projektowania systemu przetwarzania, jak i podczas samego przetwarzania, w celu zapewnienia bezpieczeństwa, a tym samym niedopuszczenia do niedozwolonego przetwarzania danych oraz zagwarantowania ochrony danych osobowych przed przypadkowym lub nielegalnym zniszczeniem lub przypadkową utratą, zmianą, niedozwolonym ujawnieniem lub dostępem.

(6) W celu ułatwienia procesu wydawania certyfikatów organizatorzy powinni korzystać z oprogramowania zapewnianego przez Komisję zgodnie z art. 6 ust. 2 rozporządzenia (UE) nr 211/2011.

(7) Podczas gromadzenia deklaracji poparcia *on-line* organizatorzy inicjatyw obywatelskich, jako administratorzy danych, powinni wdrażać wymogi specyfikacji technicznych określonych w niniejszym rozporządzeniu w celu zapewnienia ochrony przetwarzanych danych osobowych. W przypadku przetwarzania danych przez przetwarzającego organizatorzy powinni dopilnować, aby działał on wyłącznie na polecenie organizatorów i wdrażał wymogi specyfikacji technicznych określonych w niniejszym rozporządzeniu.

(8) Niniejsze rozporządzenie uwzględnia prawa podstawowe i jest zgodne z zasadami zapisanymi w Karcie praw podstawowych Unii Europejskiej, w szczególności jej art. 8, który stanowi, że każdy ma prawo do ochrony danych osobowych, które go dotyczą.

(9) Środki przewidziane w niniejszym rozporządzeniu są zgodne z opinią komitetu powołanego na mocy art. 20 rozporządzenia (UE) nr 211/2011,

[1] Dz.U. L 65 z 11.3.2011, s. 1.

[2] Dz.U. L 281 z 23.11.1995, s. 31.

PRZYJMUJE NINIEJSZE ROZPORZĄDZENIE:

Artykuł 1

Specyfikacje techniczne, o których mowa w art. 6 ust. 5 rozporządzenia (UE) nr 211/2011, są określone w załączniku.

Artykuł 2

Niniejsze rozporządzenie wchodzi w życie dwudziestego dnia po jego opublikowaniu w *Dzienniku Urzędowym Unii Europejskiej*.

Niniejsze rozporządzenie wiąże w całości i jest bezpośrednio stosowane we wszystkich państwach członkowskich.

Sporządzono w Brukseli dnia 17 listopada 2011 r.

W imieniu Komisji
José Manuel BARROSO
Przewodniczący

ZAŁĄCZNIK

1. SPECYFIKACJE TECHNICZNE DOTYCZĄCE WYKONANIA ART. 6 UST. 4 LIT. a) ROZPORZĄDZENIA (UE) NR 211/2011

W celu niedopuszczenia do składania deklaracji poparcia przez automaty przed złożeniem deklaracji w systemie sygnatariusz przechodzi odpowiedni proces weryfikacji zgodny z aktualną praktyką. Jednym z możliwych procesów weryfikacji jest zastosowanie silnego zabezpieczenia typu „captcha".

2. SPECYFIKACJE TECHNICZNE DOTYCZĄCE WYKONANIA ART. 6 UST. 4 LIT. b) ROZPORZĄDZENIA (UE) NR 211/2011

Normy dotyczące zabezpieczania informacji

2.1. Organizatorzy przedstawiają dokumentację wykazującą, że spełniają wymogi normy ISO/IEC 27001 bez konieczności przyjęcia jej. W tym celu:

a) przeprowadzili kompleksową ocenę ryzyka, obejmującą rozpoznanie systemu, wpływ na działalność operacyjną w razie wystąpienia różnych naruszeń bezpieczeństwa informacji, stworzenie listy zagrożeń i luk systemu informatycznego, opracowanie analizy zagrożeń wraz z wykazem środków mających przeciwdziałać zagrożeniom oraz środków zaradczych przewidzianych do zastosowania w przypadku wystąpienia zagrożenia, a także sporządzenie hierarchicznego wykazu udoskonaleń;

b) opracowali i wprowadzili środki służące eliminacji zagrożeń związanych z ochroną danych osobowych oraz ochroną życia rodzinnego i prywatnego, a także środków, które zostaną podjęte w razie wystąpienia zagrożenia;

c) określili na piśmie ryzyko szczątkowe;

d) zapewnili środki organizacyjne służące uzyskiwaniu informacji zwrotnych o nowych zagrożeniach i udoskonaleniach zwiększających bezpieczeństwo.

2.2. Organizatorzy dokonują wyboru środków kontroli bezpieczeństwa na podstawie analizy ryzyka, o której mowa w pkt 2.1.a), spośród następujących norm:

1) ISO/IEC 27002; lub

2) standardu dobrej praktyki opracowanego przez organizację Information Security Forum;

w celu rozwiązywania następujących kwestii:

a) ocen ryzyka (zalecana jest metodyka przewidziana w normie ISO/IEC 27005 lub inna odpowiednia do tego celu metodyka oceny ryzyka);

b) bezpieczeństwa fizycznego i bezpieczeństwa środowiska;

c) bezpieczeństwa zasobów ludzkich;

d) komunikacji i zarządzania operacyjnego;

e) standardowych środków kontroli dostępu, oprócz tych określonych w niniejszym rozporządzeniu wykonawczym;

f) pozyskiwania, rozwoju i utrzymania systemów informatycznych;

g) zarządzania incydentami związanymi z bezpieczeństwem informacji;

h) środkami zaradczymi i środkami mającymi łagodzić skutki takich naruszeń systemów informatycznych, które wiążą się ze zniszczeniem lub przypadkową utratą, zmianą, niedozwolonym ujawnieniem lub dostępem do przetwarzanych danych osobowych;

i) zgodności z wymogami;

j) bezpieczeństwa sieci komputerowych (zalecana norma ISO/IEC 27033 lub standard dobrej praktyki SoGP).

Stosowanie tych norm może być ograniczone do tych części organizacji, które są związane z systemem zbierania deklaracji *on-line*. Przykładowo, bezpieczeństwo zasobów ludzkich może ograniczać się do pracowników mających fizyczny lub sieciowy dostęp do systemu zbierania deklaracji *on-line*, a bezpieczeństwo fizyczne i środowiskowe może ograniczać się do budynków, w których znajdują się urządzenia hostingowe systemu.

Wymagania funkcjonalne

2.3. System zbierania deklaracji *on-line* składa się z instancji aplikacji sieciowej utworzonej do celów gromadzenia deklaracji poparcia dla pojedynczej inicjatywy obywatelskiej.

2.4. Jeśli administrowanie systemem wymaga różnych ról, tworzy się różne poziomy kontroli dostępu ustalane zgodnie z zasadą przydzielania jak najmniejszych uprawnień.

2.5. Publicznie dostępne funkcje są wyraźnie oddzielone od funkcji przeznaczonych do celów administracyjnych. Żadne środki kontroli dostępu nie utrudniają odczytania informacji dostępnych w publicznej części systemu, włącznie z informacjami dotyczącymi inicjatywy i elektronicznym formularzem deklaracji poparcia. Przystąpienie do inicjatywy jest możliwe tylko za pośrednictwem publicznej części systemu.

2.6. System wykrywa i uniemożliwia ponowne złożenie deklaracji poparcia.

Bezpieczeństwo na poziomie aplikacji

2.7. System jest odpowiednio zabezpieczony przed znanymi lukami w zabezpieczeniach i programami wykorzystującymi takie luki. W związku z tym spełnia on m.in. następujące wymagania:

2.7.1. System zapewnia ochronę przed iniekcją błędów poprzez zapytania z wykorzystaniem języka SQL (Structured Query Language), protokołu LDAP (Lightweight Directory Access Protocol) lub języka XPath (XML Path Language), poleceń systemu operacyjnego lub argumentów programów. W tym celu system wymaga co najmniej:

a) sprawdzania poprawności wszystkich danych wprowadzanych przez użytkowników;

b) sprawdzania poprawności przynajmniej przez mechanizmy logiczne po stronie serwera;

c) aby jakiekolwiek stosowanie interpreterów wiązało się z wyraźnym oddzieleniem niezaufanych danych pochodzących z polecenia lub zapytania. W przypadku połączeń SQL oznacza to wykorzystywanie powiązanych zmiennych we wszystkich opracowywanych deklaracjach i zachowanych procedurach oraz unikanie zapytań dynamicznych.

2.7.2. System zapewnia ochronę przed iniekcją skryptów z innych witryn (atakami XSS). W tym celu system wymaga co najmniej, by:

a) wszystkie dane wprowadzone przez użytkowników wysyłane z powrotem do przeglądarki były sprawdzane pod kątem bezpieczeństwa (poprzez weryfikację poprawności danych wejściowych);

b) wszystkie dane wprowadzone przez użytkowników były odpowiednio zmieniane przed umieszczeniem na stronie wyjściowej;

c) odpowiednie kodowanie danych wyjściowych gwarantowało traktowanie takich danych jako tekstu w przeglądarce oraz aby nie wykorzystywano żadnych aktywnych treści.

2.7.3. System posiada silne uwierzytelnianie i zarządzanie sesją, co wymaga co najmniej spełnienia poniższych warunków:

a) dane uwierzytelniające są zawsze chronione podczas przechowywania poprzez stosowanie skrótów lub szyfrowanie. Ryzyko, że ktoś uwierzytelni się za pomocą przejętego skrótu (ataku „pass-the-hash"), jest ograniczone;

b) danych uwierzytelniających nie można odgadnąć ani zastąpić, wykorzystując niedoskonałe funkcje zarządzania kontem (np. funkcje tworzenia kont, zmiany hasła, odzyskiwania hasła, słabe identyfikatory sesji);

c) identyfikatory sesji i dane sesji nie są ujawniane w adresie URL;

d) identyfikatory sesji nie są narażone na ataki z wykorzystaniem spreparowanych stałych identyfikatorów sesji (ataki typu „session fixation");

e) identyfikatory sesji mają limit czasu, który zapewnia wylogowanie użytkowników;

f) nie występuje rotacja identyfikatorów sesji po udanym logowaniu;

g) hasła, identyfikatory sesji i inne dane uwierzytelniające są przesyłane wyłącznie za pomocą protokołu TLS (Transport Layer Security);

h) część administracyjna systemu jest chroniona. Jeśli jej ochrona jest zapewniana poprzez uwierzytelnianie z wykorzystaniem jednego składnika, wówczas hasło składa się z co najmniej 10 znaków, w tym co najmniej jednej litery, jednej cyfry i jednego znaku specjalnego. Istnieje również możliwość zastosowania uwierzytelniania dwuskładnikowego. W przypadku zastosowania uwierzytelniania z wykorzystaniem jednego składnika obejmuje ono mechanizm dwuetapowej weryfikacji dostępu do części administracyjnej systemu przez internet, w którym jednemu składnikowi towarzyszy inny sposób uwierzytelniania, np. przesłanie jednorazowego hasła bądź kodu za pośrednictwem wiadomości SMS lub asymetrycznie szyfrowany losowy łańcuch znaków, który musi zostać odszyfrowany przy użyciu nieznanego dla systemu, prywatnego klucza organizatorów/administratorów.

2.7.4. System nie zawiera niezabezpieczonych bezpośrednich odniesień do obiektu. W tym celu wymagane jest co najmniej spełnienie następujących warunków:

a) w przypadku bezpośrednich odniesień do zastrzeżonych zasobów aplikacja sprawdza, czy użytkownik ma prawo dostępu do danego zasobu danych;

b) w przypadku odniesień pośrednich mapowanie do bezpośredniego odniesienia ogranicza się do wartości dopuszczalnych dla bieżącego użytkownika.

2.7.5. System posiada zabezpieczenia przed atakami CSRF (cross-site request forgery).

2.7.6. Wprowadzono właściwą konfigurację zabezpieczeń, co oznacza spełnienie co najmniej poniższych wymogów:

a) przeprowadzono aktualizację wszystkich składników oprogramowania, włącznie z systemem operacyjnym, serwerem aplikacji/WWW, systemem zarządzania bazą danych (SZBD), aplikacjami i wszystkimi bibliotekami kodów;

b) zbędne usługi systemu operacyjnego i serwera aplikacji/WWW są wyłączone, usunięte lub nie zostały zainstalowane;

c) domyślne hasła do kont zostały zmienione lub wyłączone;

d) obsługa błędów została skonfigurowana tak, aby zapobiegać przeciekom śladów stosów i innych komunikatów o błędzie mających charakter informacyjny;

e) ustawienia zabezpieczeń w strukturach programistycznych i bibliotekach zostały skonfigurowane zgodnie z najlepszą praktyką, np. wytycznymi OWASP.

2.7.7. System przewiduje szyfrowanie danych w następujący sposób:

a) dane osobowe w formie elektronicznej są szyfrowane podczas ich przechowywania lub przekazywania właściwym organom państw członkowskich zgodnie z art. 8 ust. 1 rozporządzenia (UE) nr 211/2011, a zarządzanie kluczami i tworzenie ich kopii zapasowej przeprowadzane jest oddzielnie;

b) silne algorytmy i silne klucze stosowane są zgodnie z normami międzynarodowymi. Wprowadzone jest zarządzanie kluczami;

c) hasła są skracane z wykorzystaniem silnego algorytmu i odpowiedniego ciągu zaburzającego;

d) wszystkie klucze i hasła są chronione przed dostępem osób nieupoważnionych.

2.7.8. System ogranicza dostęp do adresów URL w oparciu o poziomy dostępu i uprawnienia użytkowników. W tym celu wymagane jest co najmniej spełnienie następujących warunków:

a) w przypadku zastosowania zewnętrznych mechanizmów bezpieczeństwa do uwierzytelniania i kontrolowania autoryzacji dostępu do stron muszą one być odpowiednio skonfigurowane dla każdej strony;

b) w przypadku zastosowania ochrony na poziomie kodu taka ochrona musi zostać wprowadzona dla każdej wymaganej strony.

2.7.9. System posiada odpowiednią ochronę warstwy transportowej. W tym celu stosowane są wszystkie poniższe środki lub środki zapewniające co najmniej taki sam poziom bezpieczeństwa:

a) system wymaga, aby dostęp do wszelkich poufnych zasobów był możliwy za pomocą najnowszej wersji protokołu HTTPS (Hypertext Transfer Protocol Secure), przy użyciu certyfikatów, które są ważne, nie wygasły, nie zostały cofnięte i odpowiadają wszystkim domenom wykorzystywanym przez daną witrynę;

b) system oznacza flagą bezpieczeństwa wszystkie pliki „cookie" zawierające informacje poufne;

c) serwer wymusza, aby składnik protokołu TLS obsługiwał jedynie algorytmy szyfrowania zgodne z najlepszą praktyką. Użytkownicy są informowani, że muszą włączyć w przeglądarce obsługę protokołu TLS.

2.7.10. System zapewnia ochronę przed nieważnymi przekierowaniami.

Bezpieczeństwo baz danych i integralność danych

2.8. W przypadku wykorzystywania tych samych zasobów sprzętowych i systemu operacyjnego przez systemy zbierania deklaracji *on-line* w odniesieniu do różnych inicjatyw obywatelskich systemy te nie współdzielą żadnych danych, w tym danych uwierzytelniających związanych z dostępem lub szyfrowaniem. Znajduje to dodatkowe odzwierciedlenie w ocenie ryzyka i we wprowadzonych środkach zaradczych.

2.9. Ryzyko, że ktoś uwierzytelni się w bazie danych za pomocą przejętego skrótu (ataku „pass-the-hash"), jest ograniczone.

2.10. Dostęp do danych podawanych przez sygnatariuszy ma wyłącznie administrator bazy danych / organizator.

2.11. Dane uwierzytelniające administratora, dane osobowe zebrane od sygnatariuszy i ich kopia zapasowa są zabezpieczone algorytmami silnego szyfrowania zgodnie z pkt 2.7.7.b). Dane dotyczące państwa członkowskiego, w którym zliczane będą deklaracje poparcia, daty złożenia deklaracji oraz języka, w jakim sygnatariusz złożył deklarację poparcia, mogą być jednak przechowywane w postaci niezaszyfrowanej.

2.12. Sygnatariusze mają dostęp do przesyłanych danych wyłącznie podczas sesji, w której wypełniają formularz deklaracji poparcia. Po przesłaniu formularza deklaracji poparcia sesja ta zostaje zakończona, a przesłane dane nie są już dostępne.

2.13. Dane osobowe sygnatariuszy są dostępne w systemie, w tym również w kopii zapasowej, wyłącznie w postaci zaszyfrowanej. W celu weryfikacji lub poświadczania danych przez organy krajowe zgodnie z art. 8 rozporządzenia (UE) nr 211/2011, organizatorzy mogą eksportować zaszyfrowane dane zgodnie z pkt 2.7.7.a).

2.14. Trwałość danych wprowadzonych do formularza deklaracji poparcia jest niepodzielna. Oznacza to, że po wprowadzeniu przez użytkownika wszystkich wymaganych informacji do formularza deklaracji poparcia i zatwierdzeniu decyzji o poparciu inicjatywy system albo zapisuje wszystkie dane z formularza w bazie danych, albo – w razie błędu – nie zapisuje żadnych danych. System informuje użytkownika o udanym lub nieudanym wyniku operacji.

2.15. Stosowany SZBD jest aktualizowany i stale poprawiany w celu ochrony przed programami wykorzystującymi nowo odkryte luki w zabezpieczeniach.

2.16. Prowadzone są dzienniki aktywności całego systemu. System gwarantuje możliwość prowadzenia i przechowywania dzienników inspekcji rejestrujących wyjątki i inne niżej wymienione zdarzenia związane z bezpieczeństwem aż do momentu zniszczenia danych zgodnie z art. 12 ust. 3 lub 5 rozporządzenia (UE) nr 211/2011. Dzienniki są odpowiednio zabezpieczone, np. poprzez przechowywanie na zaszyfrowanym nośniku. Organizatorzy/administratorzy regularnie sprawdzają dzienniki pod kątem podejrzanych działań. Dzienniki zawierają co najmniej:

a) daty i godziny logowania oraz wylogowania organizatorów/administratorów;

b) wykonane kopie zapasowe;

c) wszystkie zmiany i aktualizacje dokonane przez administratora bazy danych.

Bezpieczeństwo infrastruktury – umiejscowienie, infrastruktura sieciowa i środowisko serwerowe

2.17. *Bezpieczeństwo fizyczne*

Bez względu na rodzaj hostingu, urządzenie hostingowe aplikacji jest odpowiednio chronione, co oznacza:

a) kontrolę dostępu do strefy hostingowej i prowadzenie dziennika inspekcji;

b) fizyczne zabezpieczenie danych kopii zapasowych przed kradzieżą lub przypadkowym zgubieniem;

c) montaż serwera hostingowego aplikacji w szafie serwerowej.

2.18. *Bezpieczeństwo sieci*

2.18.1. System jest umieszczony na serwerze z dostępem do internetu, zainstalowany w strefie zdemilitaryzowanej i chroniony zaporą sieciową.

2.18.2. Stosowne aktualizacje i poprawki zapory sieciowej instalowane są niezwłocznie po ich wydaniu.

2.18.3. Cały ruch przychodzący i wychodzący serwera (związany z systemem zbierania deklaracji *on-line*) jest rejestrowany w dzienniku i kontrolowany z użyciem reguł zapory sieciowej. Reguły zapory blokują ruch, który nie jest potrzebny do bezpiecznego działania systemu i do administrowania nim.

2.18.4. System zbierania deklaracji *on-line* musi być umieszczony w odpowiednio chronionym roboczym segmencie sieci, oddzielonym od segmentów, na których umieszczone są systemy nierobocze, np. środowisko programistyczne lub testowe.

2.18.5. Wprowadzono następujące środki bezpieczeństwa sieci lokalnej LAN:

a) lista kontroli dostępu do warstwy 2 (L2)/zabezpieczenie przełącznika portów;

b) porty nieużywane są w przełączniku zablokowane;

c) strefa zdemilitaryzowana znajduje się w dedykowanej wirtualnej sieci lokalnej (VLAN)/LAN;

d) trunking w warstwie 2 (L2) jest wyłączony na zbędnych portach.

2.19. *Bezpieczeństwo systemu operacyjnego i serwera aplikacji/WWW*

2.19.1. Wprowadzono właściwą konfigurację zabezpieczeń obejmującą elementy wymienione w pkt 2.7.6.

2.19.2. Aplikacje mają przydzielony najniższy poziom uprawnień wymagany do ich działania.

2.19.3. Podczas dostępu administratora do panelu zarządzania w systemie zbierania deklaracji *on-line* przydzielany jest krótki limit czasu sesji (najwyżej 15 minut).

2.19.4. Niezwłocznie po wydaniu instalowane są odpowiednie aktualizacje i poprawki do systemu operacyjnego, środowiska wykonawczego aplikacji, aplikacji działających na serwerach lub narzędzi chroniących przed złośliwym oprogramowaniem.

2.19.5. Ryzyko, że ktoś uwierzytelni się w systemie za pomocą przejętego skrótu (ataku „pass-the-hash"), jest ograniczone.

2.20. *Bezpieczeństwo oprogramowania klienckiego organizatora*

W celu zapewnienia pełnego bezpieczeństwa organizatorzy podejmują poniższe środki niezbędne do zabezpieczenia narzędzia/oprogramowania klienckiego służącego do uzyskiwania dostępu do systemu zbierania deklaracji *on-line* i do administrowania nim.

2.20.1. Przy wykonywaniu zadań niezwiązanych z konserwacją (np. automatyzacji prac biurowych) użytkownicy mają przydzielony najniższy poziom uprawnień wymagany do prawidłowego działania.

2.20.2. Stosowne aktualizacje i poprawki do systemu operacyjnego, wszelkich działających aplikacji lub narzędzi chroniących przed złośliwym oprogramowaniem są instalowane niezwłocznie po ich wydaniu.

3. SPECYFIKACJE TECHNICZNE SŁUŻĄCE DO WYKONANIA ART. 6 UST. 4 LIT. c) ROZPORZĄDZENIA (UE) NR 211/2011

3.1. W odniesieniu do każdego państwa członkowskiego system zapewnia możliwość wygenerowania raportu z podaniem inicjatywy i danych osobowych sygnatariuszy podlegających weryfikacji właściwego organu danego państwa członkowskiego.

3.2. Deklaracje poparcia złożone przez sygnatariuszy mogą być eksportowane do formatu określonego w załączniku III do rozporządzenia (UE) nr 211/2011. System może ponadto pozwalać na eksportowanie deklaracji poparcia w formacie zapewniającym interoperacyjność, np. w formacie XML (Extensible Markup Language).

3.3. Eksportowane deklaracje poparcia oznaczane są jako *dystrybucja ograniczona* do danego państwa członkowskiego oraz opatrzone etykietą *dane osobowe*.

3.4. Przesyłanie eksportowanych danych do państw członkowskich drogą elektroniczną jest zabezpieczone przed podsłuchem za pomocą szyfrowania na całej drodze przesyłu danych.