II

(Akty o charakterze nieustawodawczym)

ROZPORZĄDZENIA

ROZPORZĄDZENIE WYKONAWCZE KOMISJI (UE) 2019/1799

z dnia 22 października 2019 r.

ustanawiające specyfikacje techniczne w odniesieniu do indywidualnych systemów zbierania deklaracji online na mocy rozporządzenia Parlamentu Europejskiego i Rady (UE) 2019/788 w sprawie europejskiej inicjatywy obywatelskiej

KOMISJA EUROPEJSKA,

uwzględniając Traktat o funkcjonowaniu Unii Europejskiej,

uwzględniając rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/788 z dnia 17 kwietnia 2019 r. w sprawie europejskiej inicjatywy obywatelskiej ([1]), w szczególności jego art. 11 ust. 5,

a także mając na uwadze, co następuje:

(1) Rozporządzenie (UE) 2019/788 ustanawia zmienione przepisy dotyczące europejskiej inicjatywy obywatelskiej i uchyla rozporządzenie (UE) nr 211/2011 Parlamentu Europejskiego i Rady ([2]).

(2) Rozporządzenie (UE) 2019/788 stanowi, że w odniesieniu do zbierania deklaracji poparcia dla zarejestrowanych inicjatyw obywatelskich organizatorzy muszą korzystać z centralnego systemu zbierania deklaracji online, stworzonego i obsługiwanego przez Komisję. Jednakże – w celu ułatwienia transformacji – w przypadku inicjatyw zarejestrowanych na mocy rozporządzenia (UE) 2019/788 przed końcem 2022 r. organizatorzy mogą zdecydować się na korzystanie z własnego indywidualnego systemu zbierania deklaracji online.

(3) Zgodnie z rozporządzeniem (UE) 2019/788 indywidualny system stosowany do zbierania deklaracji poparcia online powinien mieć odpowiednie cechy techniczne i cechy bezpieczeństwa w celu zapewnienia bezpiecznego zbierania, przechowywania i przekazywania danych przez cały czas trwania procedury. Komisja powinna określić we współpracy z państwami członkowskimi specyfikacje techniczne do celów wdrażania wymogów w odniesieniu do indywidualnych systemów zbierania deklaracji online.

(4) Przepisy zawarte w niniejszym rozporządzeniu zastępują przepisy zawarte w rozporządzeniu wykonawczym Komisji (UE) nr 1179/2011 ([3]), które staną się w związku z tym nieaktualne.

(5) Środki techniczne i organizacyjne, które należy wprowadzić, powinny mieć na celu zapobieganie – zarówno w momencie projektowania, jak i przez cały okres zbierania deklaracji – nieuprawnionemu przetwarzaniu danych osobowych oraz ich ochronę przed przypadkowym lub bezprawnym zniszczeniem lub przypadkową utratą, zmianą, nieuprawnionym ujawnieniem lub dostępem.

([1]) Dz.U. L 130 z 17.5.2019, s. 55.
([2]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 211/2011 z dnia 16 lutego 2011 r. w sprawie inicjatywy obywatelskiej (Dz. U. L 65 z 11.3.2011, s. 1).
([3]) Rozporządzenie wykonawcze Komisji (UE) nr 1179/2011 z dnia 17 listopada 2011 r. ustanawiające specyfikacje techniczne w odniesieniu do systemów zbierania deklaracji online na mocy rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 211/2011 w sprawie inicjatywy obywatelskiej (Dz.U. L 301 z 18.11.2011, s. 3).

(6) W tym celu organizatorzy powinni stosować odpowiednie procedury zarządzania ryzykiem, aby identyfikować zagrożenia dla ich systemów oraz określać odpowiednie i proporcjonalne środki zaradcze w celu ograniczenia tych zagrożeń do dopuszczalnego poziomu. Organizatorzy powinni właściwie dokumentować zidentyfikowane zagrożenia w zakresie bezpieczeństwa i ochrony danych oraz środki podjęte w celu przeciwdziałania tym zagrożeniom, z uwzględnieniem zasad bezpieczeństwa i wymogów stosowanych przez instytucję certyfikującą. Przepisy i wymogi w zakresie bezpieczeństwa powinny być zgodne z rozporządzeniem (UE) 2019/788 i na żądanie powinny być udostępniane przez instytucję certyfikującą.

(7) Wdrożenie specyfikacji technicznych określonych w niniejszym rozporządzeniu powinno pozostawać bez uszczerbku dla obowiązku przestrzegania przez organizatorów wymogów ochrony danych wynikających z rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 ([4]), w tym ewentualnej potrzeby przeprowadzenia oceny skutków dla ochrony danych.

(8) Przedstawiciela grupy organizatorów lub, w stosownych przypadkach, osobę prawną, o której mowa w art. 5 ust. 7 tego rozporządzenia, uznaje się za administratorów danych na mocy rozporządzenia (UE) 2016/679 w odniesieniu do przetwarzania danych osobowych w indywidualnym systemie zbierania deklaracji online.

(9) Organizatorzy, którzy wprowadzają zmiany w swoim indywidualnym systemie zbierania deklaracji online po certyfikacji systemu, powinni bez zbędnej zwłoki powiadomić o tym właściwą instytucję certyfikującą, jeżeli zmiana może wpłynąć na ocenę leżącą u podstaw certyfikacji. Przed podjęciem takiej decyzji organizatorzy mogą zwrócić się o poradę do instytucji certyfikującej w celu sprawdzenia, czy zmiana może mieć taki wpływ, i w związku z tym należy o niej powiadomić.

(10) Zgodnie z art. 42 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2018/1725 ([5]) skonsultowano się z Europejskim Rzecznikiem Ochrony Danych, który przedstawił swoje uwagi w dniu 16 września 2019 r. Przeprowadzono konsultacje z Europejską Agencją ds. Bezpieczeństwa Sieci i Informacji, która przedstawiła swoje uwagi w dniu 18 lipca 2019 r.

(11) Środki przewidziane w niniejszym rozporządzeniu są zgodne z opinią komitetu ustanowionego na mocy art. 22 rozporządzenia (UE) 2019/788,

PRZYJMUJE NINIEJSZE ROZPORZĄDZENIE:

Artykuł 1

Specyfikacje techniczne, o których mowa w art. 11 ust. 5 rozporządzenia (UE) 2019/788, są określone w załączniku do niniejszego rozporządzenia.

Artykuł 2

1. Organizatorzy zapewniają, aby ich indywidualny system zbierania deklaracji online był zgodny ze specyfikacjami technicznymi określonymi w załączniku przez cały okres zbierania deklaracji.

2. Organizatorzy powiadamiają bez zbędnej zwłoki właściwy organ państwa członkowskiego, o którym mowa w art. 11 ust. 3 rozporządzenia (UE) 2019/788, o zmianach wprowadzonych w systemie lub we wspierających środkach organizacyjnych po certyfikacji systemu przez ten organ, jeżeli zmiany te mogą mieć wpływ na ocenę leżącą u podstaw certyfikacji. Przed wprowadzeniem takich zmian organizatorzy mogą zwrócić się o poradę do właściwego organu w celu sprawdzenia, czy dana zmiana może mieć taki wpływ.

([4]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.U. L 119 z 4.5.2016, s. 1).

([5]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1725 z dnia 23 października 2018 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje, organy i jednostki organizacyjne Unii i swobodnego przepływu takich danych oraz uchylenia rozporządzenia (WE) nr 45/2001 i decyzji nr 1247/2002/WE (Dz.U. L 295 z 21.11.2018, s. 39).

Artykuł 3

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

Niniejsze rozporządzenie stosuje się od dnia 1 stycznia 2020 r.

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

Sporządzono w Brukseli dnia 22 października 2019 r.

W imieniu Komisji
Jean-Claude Juncker
Przewodniczący

ZAŁĄCZNIK

1. **Specyfikacje techniczne dotyczące wykonania art. 11 ust. 4 lit. A) rozporządzenia (UE) 2019/788**

System wdraża środki techniczne w celu zapewnienia, by deklaracje poparcia mogły składać tylko osoby fizyczne. Środki techniczne nie wymagają gromadzenia i przechowywania większej ilości danych osobowych niż dane wymienione w załączniku III do rozporządzenia (UE) 2019/788.

2. **Specyfikacje techniczne dotyczące wykonania art. 11 ust. 4 lit. B) rozporządzenia (UE) 2019/788**

Organizatorzy wprowadzają odpowiednie i skuteczne środki techniczne i organizacyjne w celu zarządzania ryzykiem związanym z bezpieczeństwem sieci i systemów informatycznych, z których korzystają w swoich operacjach, w celu zapewnienia, by informacje podane na temat inicjatywy w systemie zbierania deklaracji online i przedstawione publicznie w internecie odpowiadały informacjom opublikowanym na temat danej inicjatywy w rejestrze, o którym mowa w art. 6 ust. 5 rozporządzenia (UE) 2019/788.

Organizatorzy zapewniają, by:

a) informacje podane na temat inicjatywy w systemie zbierania deklaracji online były zgodne z informacjami opublikowanymi w rejestrze;

b) system przedstawiał informacje na temat inicjatywy opublikowane w rejestrze, zanim obywatel złoży deklarację poparcia;

c) wdrożono środki bezpieczeństwa mające na celu zagwarantowanie, aby pola wprowadzania danych w deklaracjach poparcia były przedstawiane wraz z informacjami na temat danej inicjatywy, aby uniknąć ryzyka, że deklaracje poparcia zostaną przedłożone w ramach innej inicjatywy poprzez wprowadzenie w błąd w odniesieniu do danej inicjatywy;

d) system gwarantował, że po wprowadzeniu danych w deklaracjach poparcia zostaną one zapisane wraz z informacjami na temat danej inicjatywy;

e) zastosowano środki bezpieczeństwa uniemożliwiające nieuprawnione wprowadzanie zmian do informacji podanych na temat danej inicjatywy w systemie zbierania deklaracji online.

3. **Specyfikacje techniczne dotyczące wykonania art. 11 ust. 4 lit. C) rozporządzenia (UE) 2019/788**

System zapewnia składanie deklaracji poparcia zgodnie z polami danych zawartymi w załączniku III do rozporządzenia (UE) 2019/788.

System zapewnia, by dana osoba mogła złożyć deklarację poparcia dopiero po potwierdzeniu, że zapoznała się z oświadczeniem o ochronie prywatności zawartym w załączniku III do rozporządzenia (UE) 2019/788.

4. **Specyfikacje techniczne dotyczące wykonania art. 11 ust. 4 lit. D) rozporządzenia (UE) 2019/788**

4.1. **Zarządzanie**

4.1.1. Grupa organizatorów mianuje specjalistę ds. bezpieczeństwa odpowiedzialnego za bezpieczeństwo systemu i bezpieczne przekazywanie zgromadzonych deklaracji poparcia do właściwego organu odpowiedzialnego państwa członkowskiego. Specjalista ds. bezpieczeństwa nadzoruje procesy zabezpieczania informacji oraz techniczne i organizacyjne środki bezpieczeństwa w celu zapewnienia bezpiecznego gromadzenia, przechowywania i przekazywania danych dostarczonych przez sygnatariuszy.

4.1.2. Organizatorzy mogą zwrócić się do właściwego organu krajowego, o którym mowa w art. 11 ust. 3 rozporządzenia (UE) 2019/788, o przedstawienie mających zastosowanie zasad i wymogów bezpieczeństwa dotyczących certyfikacji indywidualnych systemów zbierania deklaracji online. Właściwy organ przedstawia te zasady i wymogi bezpieczeństwa zasadniczo w terminie jednego miesiąca od otrzymania wniosku. Mające zastosowanie zasady i wymogi bezpieczeństwa są zgodne z istniejącymi odpowiednimi krajowymi lub międzynarodowymi normami bezpieczeństwa.

4.1.3. Zasady i wymogi bezpieczeństwa dotyczące certyfikacji systemu odnoszą się do ryzyka określonego w pkt 4.2 i uwzględniają specyfikacje określone w pkt 4.3.

4.2. **Zabezpieczanie informacji**

4.2.1. Organizatorzy stosują procesy zarządzania ryzykiem w celu określenia ryzyka związanego z korzystaniem z ich systemów, w tym w odniesieniu do praw i swobód sygnatariuszy, oraz w celu określenia odpowiednich i proporcjonalnych środków mających na celu zapobieganie incydentom wpływającym na bezpieczeństwo sieci i systemów informatycznych wykorzystywanych w ich operacjach.

Proces zarządzania ryzykiem koncentruje się w szczególności na ryzyku związanym z poufnością i integralnością informacji w systemie. Ryzyko to może wynikać z zagrożeń, w tym:

a) błędów użytkownika;

b) błędów administratora systemu/bezpieczeństwa;

c) błędów konfiguracji;

d) zakażenia złośliwym oprogramowaniem;

e) przypadkowej zmiany informacji;

f) ujawnienia lub wycieków informacji;

g) podatności oprogramowania na zagrożenia;

h) nieuprawnionego dostępu;

i) przechwycenia lub podsłuchiwania ruchu internetowego;

j) ryzyka w zakresie ochrony danych.

4.2.2. Organizatorzy przedstawiają dokumentację potwierdzającą, że:

a) ocenili ryzyko systemu;

b) określili odpowiednie środki mające na celu zapobieganie incydentom mającym wpływ na bezpieczeństwo systemu oraz łagodzenie ich skutków;

c) zidentyfikowali ryzyko rezydualne;

d) wdrożyli odnośne środki i zweryfikowali ich wdrożenie;

e) zapewnili środki organizacyjne służące uzyskiwaniu informacji o nowych zagrożeniach i udoskonaleniach zwiększających bezpieczeństwo;

f) w trakcie całego procesu gromadzenia danych spełniają wymogi w zakresie certyfikacji określone w art. 11 ust. 4 rozporządzenia (UE) 2019/788, w tym wprowadzili niezbędne procesy zapewniające ich spełnienie.

4.2.3. Środki mające na celu zapobieganie incydentom wpływającym na bezpieczeństwo systemów oraz łagodzenie ich skutków obejmują następujące dziedziny:

a) bezpieczeństwo zasobów ludzkich;

b) kontrola dostępu;

c) środki kontroli kryptograficznej;

d) bezpieczeństwo fizyczne i bezpieczeństwo środowiska;

e) bezpieczeństwo operacji;

f) bezpieczeństwo łączności;

g) zakup, rozwój i utrzymanie systemu;

h) zarządzanie incydentami związanymi z bezpieczeństwem informacji;

i) zgodność.

Stosowanie tych środków bezpieczeństwa może być ograniczone do tych części danej organizacji, które są związane z systemem zbierania deklaracji online. Przykładowo, bezpieczeństwo zasobów ludzkich może ograniczać się do pracowników mających fizyczny lub zdalny dostęp do systemu zbierania deklaracji online, a bezpieczeństwo fizyczne i środowiskowe może ograniczać się do budynków, w których znajdują się urządzenia hostingowe systemu.

4.2.4. W przypadku gdy organizatorzy korzystają z podmiotu przetwarzającego w celu opracowania lub wdrożenia systemów zbierania deklaracji online lub ich części, organizatorzy przedstawiają dokumentację umożliwiającą instytucji certyfikującej sprawdzenie, czy wprowadzono niezbędne środki kontroli bezpieczeństwa.

4.3. **Szyfrowanie danych**

System zapewnia następujące szyfrowanie danych:

a) dane osobowe w formie elektronicznej są szyfrowane podczas ich przechowywania lub przekazywania właściwym organom państw członkowskich zgodnie z rozporządzeniem (UE) 2019/788, a zarządzanie kluczami i tworzenie ich kopii zapasowej realizowane jest oddzielnie;

b) stosuje się odpowiednie standardowe algorytmy i odpowiednie klucze zgodnie z normami międzynarodowymi (takimi jak norma ETSI). wprowadzono zarządzanie kluczami;

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