Dziennik Urzędowy
Unii Europejskiej

PL
Seria L

2025/2160

28.10.2025

ROZPORZĄDZENIE WYKONAWCZE KOMISJI (UE) 2025/2160

z dnia 27 października 2025 r.

ustanawiające zasady stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 w odniesieniu do norm referencyjnych, specyfikacji i procedur dotyczących zarządzania ryzykiem związanym ze świadczeniem niekwalifikowanych usług zaufania

KOMISJA EUROPEJSKA,

uwzględniając Traktat o funkcjonowaniu Unii Europejskiej,

uwzględniając rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE ([1]), w szczególności jego art. 19a ust. 2,

a także mając na uwadze, co następuje:

(1) Niekwalifikowani dostawcy usług zaufania odgrywają ważną rolę w środowisku cyfrowym, świadcząc usługi zaufania, które ułatwiają bezpieczne transakcje elektroniczne. Rozporządzenie (UE) nr 910/2014 nakłada mniej wymogów regulacyjnych na niekwalifikowanych dostawców usług zaufania niż na kwalifikowanych dostawców usług zaufania. Wszyscy dostawcy usług zaufania podlegają jednak wymogom dotyczącym bezpieczeństwa i odpowiedzialności, aby zapewnić należytą staranność, przejrzystość i rozliczalność wykonywanych przez nich operacji i świadczonych przez nich usług.

(2) Niekwalifikowanych dostawców usług zaufania można uznać za podmioty ważne lub kluczowe zgodnie z art. 3 dyrektywy Parlamentu Europejskiego i Rady (UE) 2022/2555 ([2]). W związku z tym zastosowanie ma do nich rozporządzenie wykonawcze Komisji (UE) 2024/2690 ([3]) ustanawiające wymogi techniczne i metodyczne dotyczące środków zarządzania ryzykiem w cyberbezpieczeństwie. Zakres wymogów określonych w art. 19a ust. 1 lit. a) rozporządzenia (UE) nr 910/2014 odnosi się jednak do procedur zarządzania ryzykiem dotyczących ryzyka prawnego, biznesowego, operacyjnego oraz innego bezpośredniego lub pośredniego ryzyka dla świadczenia niekwalifikowanych usług zaufania. Aby uzupełnić ramy zarządzania ryzykiem określone w rozporządzeniu wykonawczym (UE) 2024/2690 oraz umożliwić spójne podejście do zarządzania wszystkimi odpowiednimi rodzajami ryzyka, należy ustanowić specyfikacje i procedury dotyczące zarządzania tym ryzykiem przez niekwalifikowanych dostawców usług zaufania. W opracowywaniu i wdrażaniu odpowiednich polityk zarządzania ryzykiem niekwalifikowanych dostawców usług zaufania mogą wspierać wytyczne Agencji Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA) lub właściwych organów krajowych wydane na podstawie dyrektywy (UE) 2022/2555.

([1]) Dz.U. L 257 z 28.8.2014, s. 73, ELI: http://data.europa.eu/eli/reg/2014/910/oj.

([2]) Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (dyrektywa NIS 2) (Dz.U. L 333 z 27.12.2022, s. 80, ELI: http://data.europa.eu/eli/dir/2022/2555/oj).

([3]) Rozporządzenie wykonawcze Komisji (UE) 2024/2690 z dnia 17 października 2024 r. ustanawiające zasady stosowania dyrektywy (UE) 2022/2555 w odniesieniu do wymogów technicznych i metodycznych dotyczących środków zarządzania ryzykiem w cyberbezpieczeństwie oraz doprecyzowujące przypadki, w których incydent uznaje się za poważny w odniesieniu do dostawców usług DNS, rejestrów nazw TLD, dostawców usług chmurowych, dostawców usług ośrodka przetwarzania danych, dostawców sieci dostarczania treści, dostawców usług zarządzanych, dostawców usług zarządzanych w zakresie bezpieczeństwa, dostawców internetowych platform handlowych, wyszukiwarek internetowych i platform usług sieci społecznościowych oraz dostawców usług zaufania (Dz.U. L, 2024/2690, 18.10.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/2690/oj).

(3) Domniemanie zgodności określone w art. 19a ust. 2 rozporządzenia (UE) nr 910/2014 powinno mieć zastosowanie wyłącznie w przypadku, gdy niekwalifikowani dostawcy usług zaufania spełniają wymogi określone w niniejszym rozporządzeniu. Normy referencyjne, o których mowa w załączniku, powinny odzwierciedlać utrwalone praktyki i być powszechnie uznawane w odpowiednich sektorach. W celu zapewnienia, aby niekwalifikowani dostawcy usług zaufania zarządzali ryzykiem prawnym, biznesowym, operacyjnym oraz innymi bezpośrednimi lub pośrednimi ryzykami dla świadczenia niekwalifikowanej usługi zaufania zgodnie z art. 19a ust. 1 rozporządzenia (UE) nr 910/2014, powinni oni przestrzegać przywołanych elementów norm określonych w załączniku oraz wymogów w zakresie zarządzania ryzykiem określonych w niniejszym rozporządzeniu w odniesieniu do domniemania zgodności.

(4) Jeżeli niekwalifikowany dostawca usług zaufania spełnia wymogi określone w niniejszym rozporządzeniu wykonawczym, organy nadzoru powinny zakładać zgodność z odpowiednimi wymogami rozporządzenia (UE) nr 910/2014. Niekwalifikowany dostawca usług zaufania może jednak nadal opierać się na innych praktykach w celu wykazania zgodności z wymogami rozporządzenia (UE) nr 910/2014.

(5) Aby zapewnić odpowiednie uwzględnienie zidentyfikowanego ryzyka, polityka zarządzania ryzykiem stosowana przez niekwalifikowanych dostawców usług zaufania powinna obejmować procedury dokumentowania i oceny ryzyka, a także określania, wyboru i wdrażania odpowiednich środków postępowania z ryzykiem. Wdrażanie środków postępowania z ryzykiem powinno być stale monitorowane. W odniesieniu do informacji, które niekwalifikowani dostawcy usług zaufania rejestrują i przechowują w ramach swoich środków postępowania z ryzykiem, dostawcy ci powinni zapewnić integralność i poufność danych. Ponadto, aby zwiększyć przejrzystość i wspierać działania nadzorcze, niekwalifikowani dostawcy usług zaufania powinni publikować stosowane przez siebie metody weryfikacji tożsamości. Z uwagi na fakt, że nie wszystkie zidentyfikowane rodzaje ryzyka można w pełni wyeliminować poprzez ich unikanie, ograniczanie lub przenoszenie na inne podmioty, wszelkie ryzyko rezydualne powinny zatwierdzać organy zarządzające niekwalifikowanych dostawców usług zaufania. Kryteria akceptacji ryzyka rezydualnego powinny być uzasadnione w zrozumiały sposób.

(6) Komisja regularnie przeprowadza ocenę nowych technologii, praktyk, norm lub specyfikacji technicznych. Zgodnie z motywem 75 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2024/1183 ([4]) Komisja powinna poddawać przeglądowi i w razie potrzeby aktualizować niniejsze rozporządzenie wykonawcze, aby zachować jego aktualność względem globalnych zmian, nowych technologii, praktyk, norm lub specyfikacji technicznych oraz nadążać za najlepszymi praktykami na rynku wewnętrznym.

(7) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 ([5]) oraz – w stosownych przypadkach – dyrektywa 2002/58/WE Parlamentu Europejskiego i Rady ([6]) mają zastosowanie do wszystkich czynności przetwarzania danych osobowych na podstawie niniejszego rozporządzenia.

(8) Zgodnie z art. 42 ust. 1 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2018/1725 ([7]) skonsultowano się z Europejskim Inspektorem Ochrony Danych, który wydał opinię w dniu 8 sierpnia 2025 r. ([8]).

([4]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/1183 z dnia 11 kwietnia 2024 r. w sprawie zmiany rozporządzenia (UE) nr 910/2014 w odniesieniu do ustanowienia europejskich ram tożsamości cyfrowej (Dz.U. L, 2024/1183, 30.4.2024, ELI: http://data.europa.eu/eli/reg/2024/1183/oj).

([5]) 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, ELI: http://data.europa.eu/eli/reg/2016/679/oj).

([6]) Dyrektywa 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. dotycząca przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (dyrektywa o prywatności i łączności elektronicznej) (Dz.U. L 201 z 31.7.2002, s. 37, ELI: http://data.europa.eu/eli/dir/2002/58/oj).

([7]) 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, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

([8]) Formalne uwagi EIOD do projektu rozporządzenia wykonawczego w odniesieniu do specyfikacji i procedur zarządzania ryzykiem związanym ze świadczeniem niekwalifikowanych usług zaufania | Europejski Inspektor Ochrony Danych.

(9) Środki przewidziane w niniejszym rozporządzeniu są zgodne z opinią komitetu ustanowionego na podstawie art. 48 rozporządzenia (UE) nr 910/2014,

PRZYJMUJE NINIEJSZE ROZPORZĄDZENIE:

Artykuł 1

Normy referencyjne

Normy referencyjne, o których mowa w art. 19a ust. 2 rozporządzenia (UE) nr 910/2014, określono w załączniku do niniejszego rozporządzenia.

Artykuł 2

Polityki zarządzania ryzykiem

1. Polityki zarządzania ryzykiem, o których mowa w art. 19a ust. 1 rozporządzenia (UE) nr 910/2014, wyraźnie określają usługi zaufania, do których mają zastosowanie, dotyczą określonych usług zaufania i zatwierdza je organ zarządzający niekwalifikowanego dostawcy usług zaufania.

2. Polityki zarządzania ryzykiem obejmują co najmniej wszystkie następujące elementy:

a) ogólny poziom tolerancji ryzyka zgodnie z krytycznością i wymaganym poziomem bezpieczeństwa usług zaufania, z uwzględnieniem najnowszych osiągnięć technologicznych;

b) odpowiednie kryteria ryzyka, w tym co najmniej prawdopodobieństwo, wpływ i poziom ryzyka, z uwzględnieniem analizy zagrożeń cyberbezpieczeństwa i podatności na nie;

c) podejście do identyfikacji i dokumentowania ryzyka związanego ze świadczeniem usług zaufania, z uwzględnieniem pełnego zakresu systemu informacyjnego wykorzystywanego przez niekwalifikowanego dostawcę usług zaufania, w tym ryzyka związanego z elementami systemu, a także z wszelkimi aktywnymi lub biernymi stronami zaangażowanymi we wdrażanie systemu lub w świadczenie usług zaufania;

d) proces oceny zidentyfikowanego ryzyka w oparciu o kryteria ryzyka, o których mowa w lit. b);

e) proces identyfikacji, szeregowania pod względem ważności i stałego monitorowania wdrażania odpowiednich środków postępowania z ryzykiem;

f) proces stałego monitorowania wdrażania polityk zarządzania ryzykiem.

3. Niekwalifikowani dostawcy usług zaufania ustanawiają odpowiednie procedury i przechowują dokumenty w celu zapewnienia wdrożenia wymogów określonych w mających zastosowanie przepisach.

4. Niekwalifikowani dostawcy usług zaufania ustanawiają odpowiednie udokumentowane procedury zapewniające monitorowanie unijnych i krajowych zmian ustawodawczych i regulacyjnych, które mogą mieć wpływ na świadczenie usług zaufania.

Artykuł 3

Identyfikacja, dokumentowanie i ocena ryzyka

Niekwalifikowani dostawcy usług zaufania identyfikują, dokumentują i oceniają wszystkie rodzaje ryzyka, o których mowa w art. 19a ust. 1 rozporządzenia (UE) nr 910/2014, zgodnie z politykami zarządzania ryzykiem, o których mowa w art. 2, a w szczególności:

a) identyfikują ryzyko związane z osobami trzecimi;

b) identyfikują potencjalny pojedynczy punkt awarii w świadczeniu usług zaufania;

c) przeprowadzają ocenę zidentyfikowanego ryzyka w oparciu o kryteria ryzyka, o których mowa w art. 2 ust. 2 lit. b).

Artykuł 4

Środki postępowania z ryzykiem

1. Zgodnie z polityką, o której mowa w art. 2, niekwalifikowani dostawcy usług zaufania planują, dokumentują i wdrażają środki postępowania z ryzykiem, a w szczególności wykonują następujące zadania:

a) określają i szeregują pod względem ważności odpowiednie środki postępowania z ryzykiem;

b) wybierają, zatwierdzają i dokumentują wybrane środki postępowania z ryzykiem – w tym związane z nimi wymogi bezpieczeństwa i procedury operacyjne – w planie postępowania z ryzykiem, określają, kto jest odpowiedzialny za wdrażanie środków postępowania z ryzykiem i kiedy należy je wdrożyć;

c) stale monitorują wdrażanie środków postępowania z ryzykiem.

2. Plan postępowania z ryzykiem przedstawiony w ust. 1 lit. b) przedstawia w zrozumiały sposób powody uzasadniające akceptację ryzyka rezydualnego.

3. Ponadto w ramach środków postępowania z ryzykiem, o których mowa w ust. 1, niekwalifikowani dostawcy usług zaufania:

a) w stosownych przypadkach weryfikują bezpośrednio lub za pośrednictwem osoby trzeciej tożsamość użytkowników usługi zaufania oraz publikują informacje na temat stosowanych metod weryfikacji tożsamości;

b) do celów dostarczenia dowodów w postępowaniu sądowym oraz zapewnienia ciągłości usług, zapisują i bezpiecznie przechowują – tak długo, jak jest to konieczne zgodnie z prawem Unii lub prawem krajowym, w tym po zaprzestaniu działalności przez niekwalifikowanego dostawcę usług zaufania – następujące informacje:

   — wszystkie istotne informacje zgromadzone w procesie rejestracji użytkowników usług zaufania i włączania ich do korzystania z usług, w tym – w stosownych przypadkach – związane z weryfikacją tożsamości użytkowników,

   — dane uwierzytelniające przypisane użytkownikowi usługi zaufania, w stosownych przypadkach, oraz

   — wszelkie zmiany statusu certyfikatów klucza publicznego lub innych materiałów kryptograficznych wykorzystywanych do świadczenia usługi zaufania;

c) w stosownych przypadkach zapewniają, aby dane uwierzytelniające przypisane użytkownikowi usługi zaufania były niepowtarzalne.

4. Przy określaniu, wyborze, zatwierdzaniu i szeregowaniu pod względem ważności odpowiednich środków postępowania z ryzykiem niekwalifikowani dostawcy usług zaufania biorą pod uwagę następujące elementy:

a) wyniki procesu oceny ryzyka, o którym mowa w art. 3;

b) skuteczność środków postępowania z ryzykiem;

c) oceny zgodności;

d) poważne incydenty;

e) koszt wdrożenia w stosunku do oczekiwanej korzyści;

f) mającą zastosowanie odpowiednią klasyfikację aktywów;

g) analizę wszelkiego wpływu na działalność ryzyka określonego zgodnie z art. 3.

5. Organy zarządzające niekwalifikowanych dostawców usług zaufania zatwierdzają ryzyko rezydualne pozostałe po wdrożeniu środków postępowania z ryzykiem określonych w planie postępowania z ryzykiem.

6. Niekwalifikowani dostawcy usług zaufania dokonują przeglądu wyników oceny ryzyka i planu postępowania z ryzykiem w zaplanowanych odstępach czasu, a co najmniej raz w roku, a także w przypadku wystąpienia istotnych zmian w infrastrukturze, operacjach lub ryzyku lub w przypadku poważnych incydentów, a także dokumentują i – w stosownych przypadkach – aktualizują te wyniki i plany.

7. Niekwalifikowani dostawcy usług zaufania zapewniają dostępność, integralność i poufność informacji, o których mowa w ust. 3 lit. b).

Artykuł 5

Wejście w życie

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 27 października 2025 r.

W imieniu Komisji
Przewodnicząca
Ursula VON DER LEYEN

ZAŁĄCZNIK

Wykaz norm referencyjnych dla niekwalifikowanych dostawców usług zaufania

Stosuje się wymogi wynikające z następujących klauzul normy ETSI EN 319 401 V3.1.1 (2024-06): „Podpisy elektroniczne i infrastruktury zaufania (ESI); Ogólne wymagania polityki dla dostawców usług zaufania”:

5. Ocena ryzyka;
6. Polityki i praktyki;
7.1. Organizacja wewnętrzna;
7.2. Zasoby ludzkie;
7.3. Zarządzanie aktywami;
7.4. Kontrola dostępu;
7.6. Bezpieczeństwo fizyczne i środowiskowe.