Dziennik Urzędowy
Unii Europejskiej

PL
Seria L

2025/1567

30.7.2025

ROZPORZĄDZENIE WYKONAWCZE KOMISJI (UE) 2025/1567

z dnia 29 lipca 2025 r.

ustanawiające zasady stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 w odniesieniu do zarządzania kwalifikowanymi urządzeniami do składania podpisu elektronicznego na odległość i kwalifikowanymi urządzeniami do składania pieczęci elektronicznej na odległość jako kwalifikowanymi usługami 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. 29a ust. 2 i art. 39a,

a także mając na uwadze, co następuje:

(1) Kwalifikowane usługi zaufania na potrzeby zarządzania kwalifikowanymi urządzeniami do składania podpisu elektronicznego na odległość oraz zarządzania kwalifikowanymi urządzeniami do składania pieczęci elektronicznej na odległość odgrywają kluczową rolę w cyfrowym otoczeniu biznesu poprzez promowanie przejścia od tradycyjnych procesów opartych na dokumentacji papierowej do ich elektronicznych odpowiedników. Te kwalifikowane usługi zaufania przyczyniają się do bezpiecznego i wiarygodnego zarządzania tymi urządzeniami działającymi na odległość w imieniu podpisujących i składających pieczęcie w sposób gwarantujący spełnienie warunków dotyczących kwalifikowanych podpisów elektronicznych i kwalifikowanych pieczęci elektronicznych.

(2) Aby zwiększyć pewność prawa i wiarygodność kwalifikowanych usług zaufania na potrzeby zarządzania kwalifikowanymi urządzeniami do składania podpisu elektronicznego na odległość i kwalifikowanymi usługami zaufania na potrzeby zarządzania kwalifikowanymi urządzeniami do składania pieczęci elektronicznej na odległość, kwalifikowani dostawcy usług zaufania świadczący te kwalifikowane usługi powinni spełniać normy określone w niniejszym rozporządzeniu.

(3) Przedmiotowe normy powinny odzwierciedlać utrwalone praktyki i być powszechnie uznawane w odpowiednich sektorach. Należy je dostosować w taki sposób, aby obejmowały odpowiednio mechanizmy kontrolne zapewniające bezpieczeństwo i wiarygodność kwalifikowanych usług zaufania, a także zapewniające podpisującym wyłączną kontrolę, nad wykorzystaniem ich danych służących do składania podpisu elektronicznego z wysokim poziomem zaufania oraz kontrolę nad wykorzystaniem danych służących do wystawiania pieczęci elektronicznej przez podmioty składające pieczęć.

(4) Aby zapewnić adekwatne ramy czasowe na potrzeby audytu dostawców usług zaufania w odniesieniu do spełnienia nowych wymogów, niniejsze rozporządzenie powinno mieć zastosowanie po upływie 24 miesięcy od jego wejścia w życie.

(5) Komisja regularnie przeprowadza ocenę nowych technologii, praktyk, norm lub specyfikacji technicznych. Zgodnie z motywem 75 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2024/1183 [2] Komisja powinna poddawać przeglądowi i w razie potrzeby aktualizować niniejsze rozporządzenie, aby zachować jego aktualność względem globalnych zmian, nowych technologii, norm lub specyfikacji technicznych oraz nadążać za najlepszymi praktykami na rynku wewnętrznym.

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

[2] 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).

(6) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 ([3]) oraz – w stosownych przypadkach – dyrektywa 2002/58/WE Parlamentu Europejskiego i Rady ([4]) mają zastosowanie do wszystkich czynności przetwarzania danych osobowych na podstawie niniejszego rozporządzenia.

(7) Zgodnie z art. 42 ust. 1 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2018/1725 ([5]) skonsultowano się z Europejskim Inspektorem Ochrony Danych, który wydał opinię w dniu 6 czerwca 2025 r.

(8) 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 i specyfikacje referencyjne

Normy i specyfikacje referencyjne dotyczące zarządzania kwalifikowanymi urządzeniami do składania podpisu elektronicznego na odległość i kwalifikowanymi urządzeniami do składania pieczęci elektronicznej na odległość jako kwalifikowanymi usługami zaufania, o których mowa w art. 29a ust. 2 i art. 39a rozporządzenia (UE) nr 910/2014, określono w załączniku do niniejszego rozporządzenia.

Artykuł 2

Wejście w życie i rozpoczęcie stosowania

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

Niniejsze rozporządzenie stosuje się od dnia 19 sierpnia 2027 r.

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

Sporządzono w Brukseli dnia 29 lipca 2025 r.

W imieniu Komisji
Przewodnicząca
Ursula VON DER LEYEN

([3]) 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).

([4]) 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).

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

ZAŁĄCZNIK

Wykaz norm i specyfikacji referencyjnych dotyczących zarządzania kwalifikowanymi urządzeniami do składania podpisu elektronicznego na odległość i kwalifikowanymi urządzeniami do składania pieczęci elektronicznej na odległość

Norma ETSI TS 119 431-1 V1.3.1 (2024-12) („ETSI TS 119 431-1") ma zastosowanie do celów oceny zgodności z unijną polityką dotyczącą usług aplikacji serwerów obsługujących podpisy v2 zgodnie z załącznikiem A do tej normy, z następującymi dostosowaniami:

1) 2.1. Odniesienia normatywne

   — [1] ETSI EN 319 401 V3.1.1 (2024-06): „Podpisy elektroniczne i infrastruktura zaufania (ESI); Ogólne wymagania polityki dla dostawców usług zaufania".

   — [7] Europejska Grupa ds. Certyfikacji Cyberbezpieczeństwa, podgrupa ds. kryptografii: „Uzgodnione mechanizmy kryptograficzne" opublikowane przez Agencję Unii Europejskiej ds. Cyberbezpieczeństwa („ENISA") ([1]).

2) 6.1. Obowiązki związane z publikacją i repozytorium

   — OVR-6.1-04: Informacje określone w pkt OVR-6.1-01 powyżej muszą być dostępne publicznie i z różnych państw.

3) 6.4.4. Mechanizmy kontrolne dotyczące personelu

   — OVR-6.4.4-02: Dostawcy usług aplikacji serwerów obsługujących podpisy (SSASP) zatrudniają personel pełniący zaufane funkcje oraz, w stosownych przypadkach, podwykonawców pełniących zaufane funkcje, którzy posiadają niezbędną wiedzę ekspercką, doświadczenie i kwalifikacje zdobyte w ramach formalnego szkolenia i dokumenty uwierzytelniające lub doświadczenie, lub oba te elementy.

   — OVR-6.4.4-03: Zgodność z pkt OVR-6.4.4-02 obejmuje regularne (co najmniej raz na 12 miesięcy) aktualizacje dotyczące nowych zagrożeń i bieżących praktyk w zakresie bezpieczeństwa.

4) 6.4.9. Zakończenie działalności SSASP

   — OVR-6.4.9-02: Plan zakończenia działalności SSASP musi być zgodny z aktami wykonawczymi przyjętymi na podstawie art. 24 ust. 5 rozporządzenia (UE) nr 910/2014 [i.1].

5) 6.5.5. Kontrole zabezpieczeń sieci

   — OVR-6.5.5-02: Wymagany w pkt REQ-7.8-13 normy ETSI EN 319 401 [1] skan podatności przeprowadza się co najmniej raz na kwartał.

   — OVR-6.5.5-03: Zapory sieciowe należy skonfigurować tak, aby uniemożliwić wszelkie protokoły i dostępy, które nie są wymagane do funkcjonowania dostawcy usług zaufania.

6) 6.8.5. Mechanizmy kontroli kryptograficznej

   — OVR-6.8.5-01: Wprowadza się odpowiednie środki kontroli bezpieczeństwa w celu zarządzania wszelkimi technikami kryptograficznymi SSASP w całym ich cyklu życia.

   — OVR-6.8.5-02: W odniesieniu do pkt OVR-6.8.5-01 SSASP wybierają i stosują odpowiednie techniki kryptograficzne spełniające wymogi określone w uzgodnionych mechanizmach kryptograficznych zatwierdzonych przez Europejską Grupę ds. Certyfikacji Cyberbezpieczeństwa i opublikowanych przez ENISA [7].

7) Załącznik A sekcja A.3 Wymagania ogólne

   — OVR-A.3-02 [EUSPv2]: Oświadczenie dotyczące praktyk dostawcy usług zaufania musi zawierać odniesienie do certyfikacji zastosowanego kwalifikowanego urządzenia do składania podpisu zgodnie z wymogami załącznika II do rozporządzenia (UE) nr 910/2014 [i.1].

([1]) https://certification.enisa.europa.eu/publications/eucc-guidelines-cryptography_en.