2025/2532

17.12.2025

ROZPORZĄDZENIE WYKONAWCZE KOMISJI (UE) 2025/2532

z dnia 16 grudnia 2025 r.

ustanawiające zasady stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 w odniesieniu do norm referencyjnych i specyfikacji dotyczących kwalifikowanych usług archiwizacji elektronicznej

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. 45j ust. 2,

a także mając na uwadze, co następuje:

(1) Rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2024/1183 ([2]) do rozporządzenia (UE) nr 910/2014 wprowadzono wykaz nowych usług zaufania i kwalifikowanych usług zaufania, w tym kwalifikowaną usługę archiwizacji elektronicznej. Komisja ma ustanowić wykaz norm referencyjnych i, w razie potrzeby, ustanowić specyfikacje dotyczące takich usług.

(2) Archiwizacja elektroniczna to usługa służąca do odbioru, przechowywania, pobierania i usuwania danych elektronicznych i dokumentów elektronicznych, aby zapewnić ich trwałość i czytelność, a także aby zachować ich integralność, poufność i dowód pochodzenia przez cały okres ich przechowywania. Kwalifikowane usługi archiwizacji elektronicznej odgrywają kluczową rolę w cyfrowym otoczeniu biznesowym poprzez wspieranie przejścia od tradycyjnych procesów opartych na dokumentacji papierowej do ich elektronicznych odpowiedników. W celu zapewnienia, aby dane elektroniczne i dokumenty elektroniczne zachowały domniemanie integralności i pochodzenia przez okres przechowywania przez kwalifikowanego dostawcę usług zaufania, oraz aby osiągnąć wysoki poziom przejrzystości i zaufania wśród wszystkich uczestników cyklu życia informacji, konieczne jest ustanowienie wspólnego zestawu specyfikacji dla kwalifikowanych usług archiwizacji elektronicznej.

(3) Aby zwiększyć wartość dowodową, bezpieczeństwo i wiarygodność kwalifikowanych usług archiwizacji elektronicznej, w przypadku gdy podpisy elektroniczne, pieczęcie elektroniczne lub elektroniczne znaczniki czasu są wykorzystywane do tworzenia, podpisywania, opatrywania pieczęcią lub poświadczania daty i godziny, na przykład archiwizacji dowodów, zapisów dowodowych, zapisów zdarzeń, zapisów dotyczących prawidłowego wdrożenia procedur lub archiwizacji sprawozdań potwierdzających, należy korzystać z kwalifikowanych usług zaufania.

(4) Domniemanie zgodności określone w art. 45j ust. 2 rozporządzenia (UE) nr 910/2014 powinno mieć zastosowanie wyłącznie w przypadku, gdy kwalifikowane usługi archiwizacji elektronicznej spełniają wymogi określone w niniejszym rozporządzeniu. Normy referencyjne dotyczące kwalifikowanych usług archiwizacji elektronicznej powinny odzwierciedlać utrwalone praktyki i być powszechnie uznawane w odpowiednich sektorach. Należy je dostosować w taki sposób, aby obejmowały dodatkowe kontrole zapewniające bezpieczeństwo i wiarygodność kwalifikowanych usług archiwizacji elektronicznej.

(5) Jeżeli dostawca usług zaufania spełnia wymogi określone w niniejszym rozporządzeniu, organy nadzoru powinny domniemywać zgodność z odpowiednimi wymogami rozporządzenia (UE) nr 910/2014 i należycie uwzględniać takie domniemanie w odniesieniu do przyznania lub potwierdzenia statusu kwalifikowanego usługi zaufania. Kwalifikowany dostawca usług zaufania może jednak nadal polegać na innych praktykach w celu wykazania zgodności z wymogami rozporządzenia (UE) nr 910/2014.

(6) Aby zachować integralność i dowód pochodzenia danych elektronicznych i dokumentów elektronicznych zawierających jeden lub więcej kwalifikowanych podpisów lub jedną lub więcej kwalifikowanych pieczęci elektronicznych, kwalifikowane usługi archiwizacji elektronicznej powinny stosować procedury i technologie umożliwiające przedłużenie wiarygodności tych podpisów i pieczęci elektronicznych poza technologiczny okres ważności co najmniej przez cały okres przechowywania.

([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).

(7) Komisja regularnie przeprowadza ocenę nowych technologii, praktyk, norm lub specyfikacji technicznych. Zgodnie z motywem 75 rozporządzenia (UE) 2024/1183 Komisja powinna, w razie potrzeby, poddawać niniejsze rozporządzenie przeglądowi i aktualizacji, aby zachować jego aktualność względem globalnych zmian, nowych technologii, praktyk, norm lub specyfikacji technicznych oraz przestrzegać najlepszych praktyk na rynku wewnętrznym.

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

(9) 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 21 października 2025 r. ([6]).

(10) 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

Archiwizacja elektroniczna dokumentów opatrzonych kwalifikowanym podpisem elektronicznym lub kwalifikowaną pieczęcią elektroniczną

1. Przy archiwizowaniu danych elektronicznych lub dokumentów elektronicznych zawierających kwalifikowane podpisy elektroniczne lub kwalifikowane pieczęcie elektroniczne dostawcy kwalifikowanych usług archiwizacji elektronicznej zapewniają utrzymanie wiarygodności tych kwalifikowanych podpisów elektronicznych lub kwalifikowanych pieczęci elektronicznych, w tym po zakończeniu ich technologicznego okresu ważności, oraz utrzymanie integralności i dokładności pochodzenia kwalifikowanych podpisów i pieczęci elektronicznych, co najmniej do końca okresu przechowywania przewidzianego przepisami prawa lub umową.

2. Do celów ust. 1 dostawcy kwalifikowanych usług archiwizacji elektronicznej mogą polegać na kwalifikowanej usłudze konserwacji kwalifikowanych podpisów elektronicznych lub kwalifikowanej usłudze konserwacji kwalifikowanych pieczęci elektronicznych.

Artykuł 2

Normy referencyjne i specyfikacje dotyczące świadczenia kwalifikowanych usług archiwizacji elektronicznej

Normy referencyjne i specyfikacje, o których mowa w art. 45j ust. 2 rozporządzenia (UE) nr 910/2014, określono w załączniku do niniejszego rozporządzenia.

([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).

([6]) EDPS Formal comments on the draft Implementing Regulation laying down rules for the application of Regulation (EU) No 910/2014 as regards reference standards and specifications for qualified electronic archiving services [Formalne uwagi EIOD do projektu rozporządzenia wykonawczego ustanawiającego zasady stosowania rozporządzenia (UE) nr 910/2014 w odniesieniu do norm referencyjnych i specyfikacji dotyczących kwalifikowanych usług archiwizacji elektronicznej].

Artykuł 3

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 16 grudnia 2025 r.

W imieniu Komisji
Przewodnicząca
Ursula VON DER LEYEN

ZAŁĄCZNIK

Wykaz norm referencyjnych i specyfikacji dotyczących kwalifikowanych usług archiwizacji elektronicznej

Norma CEN/TS 18170:2025 („CEN/TS 18170") ma zastosowanie z następującymi dostosowaniami:

a) Odniesienia normatywne (klauzula 2)

— ETSI EN 319 401 V3.1.1 (2024-06), Podpisy elektroniczne i infrastruktura zaufania (ESI); Ogólne wymagania polityki dla dostawców usług zaufania.

— ETSI EN 319 421 V1.3.1 (2025-07), Podpisy elektroniczne i infrastruktura (ESI); Wymagania polityki i bezpieczeństwa dla dostawców usług zaufania wydających znaczniki czasu.

— ISO 14721:2025, Praktyki systemu danych pochodzących z przestrzeni kosmicznej – Model referencyjny otwartego systemu archiwizacji informacji (OAIS).

— ACM-ECCG, Europejska Grupa ds. Certyfikacji Cyberbezpieczeństwa, podgrupa ds. kryptografii: „Uzgodnione mechanizmy kryptograficzne" opublikowane przez Agencję Unii Europejskiej ds. Cyberbezpieczeństwa („ENISA").

— CIR (UE) 2024/482, rozporządzenie wykonawcze Komisji (UE) 2024/482 ([1]).

— CIR (UE) 2024/3144, rozporządzenie wykonawcze Komisji (UE) 2024/3144 ([2]).

— ISO/IEC 15408:2022 (części 1–5) „Bezpieczeństwo informacji, cyberbezpieczeństwo i ochrona prywatności – Kryteria oceny zabezpieczeń informatycznych".

— FIPS PUB 140-3 (2019) „Wymogi bezpieczeństwa dotyczące modułów kryptograficznych".

b) Polityka i oświadczenie na temat praktyk (klauzula 6.1)

— Zastosowanie mają wymagania klauzuli 6.1 normy CEN/TS 18170.

— Stosuje się wymagania określone w klauzuli 5 normy ETSI EN 319 401.

— Dostawca usług zaufania w zakresie archiwizacji elektronicznej (EATSP) ustanawia procedury powiadamiania organu nadzoru o wszelkich zmianach w świadczeniu usługi zaufania w zakresie archiwizacji elektronicznej oraz o zamiarze zaprzestania tej działalności, zgodnie z wymogami biznesowymi oraz odpowiednimi przepisami ustawowymi i wykonawczymi, w tym zgodnie z wymogami aktów wykonawczych przyjętych na podstawie art. 24 ust. 5 rozporządzenia (UE) nr 910/2014 [i.2].

— Dostawca usług zaufania w zakresie archiwizacji elektronicznej powiadamia właściwy organ nadzoru co najmniej:

  — na miesiąc przed wprowadzeniem jakiejkolwiek zmiany,

  — na trzy miesiące przed planowanym zaprzestaniem świadczenia usług zaufania.

c) Warunki korzystania z usługi (klauzula 6.2)

— Zastosowanie mają wymagania klauzuli 6.2 normy CEN/TS 18170.

— Przed nawiązaniem stosunku umownego abonenci i strony ufające korzystające z usługi zaufania w zakresie archiwizacji elektronicznej są informowani, w sposób jasny, wyczerpujący i łatwo dostępny, w publicznie dostępnej przestrzeni i indywidualnie, o dokładnych warunkach korzystania z usługi.

([1]) Rozporządzenie wykonawcze Komisji (UE) 2024/482 z dnia 31 stycznia 2024 r. ustanawiające zasady stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) 2019/881 w odniesieniu do przyjęcia europejskiego programu certyfikacji cyberbezpieczeństwa opartego na wspólnych kryteriach (EUCC) (Dz.U. L, 2024/482, 7.2.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/482/oj).

([2]) Rozporządzenie wykonawcze Komisji (UE) 2024/3144 z dnia 18 grudnia 2024 r. w sprawie zmiany rozporządzenia wykonawczego (UE) 2024/482 w odniesieniu do mających zastosowanie norm międzynarodowych i w sprawie sprostowania tego rozporządzenia wykonawczego (Dz.U. L, 2024/3144, 19.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/3144/oj).

d) Zasoby ludzkie (klauzula 7.3)

— Zastosowanie mają wymagania klauzuli 7.3 normy CEN/TS 18170.

— Personel dostawcy usług zaufania w zakresie archiwizacji elektronicznej pełniący zaufane funkcje oraz, w stosownych przypadkach, jego podwykonawcy pełniący zaufane funkcje muszą być w stanie spełnić wymóg „posiadania wiedzy eksperckiej, doświadczenia i kwalifikacji" zdobytych w ramach formalnego szkolenia i dokumentów uwierzytelniających lub doświadczenia, lub obu tych elementów. Obejmuje to regularne aktualizacje (co najmniej raz na 12 miesięcy) dotyczące nowych zagrożeń i obecnych praktyk w zakresie bezpieczeństwa.

e) Kontrole kryptograficzne i monitorowanie (klauzula 7.6)

— System archiwizacji musi gwarantować poufność danych i dokumentów przez cały cykl życia archiwum, od jego przekazania do jego usunięcia.

— Zastosowanie mają wymagania określone w klauzuli 7.5 „Kontrole kryptograficzne" normy ETSI EN 319 401.

— Dostawca usług zaufania w zakresie archiwizacji elektronicznej ustala pochodzenie danych, które mają być archiwizowane w elektronicznym systemie archiwizacji. Jeśli w tym celu wykorzystuje podpisy elektroniczne lub pieczęcie elektroniczne, te podpisy elektroniczne lub pieczęcie elektroniczne muszą być kwalifikowane.

— Jeżeli dostawca usług zaufania w zakresie archiwizacji elektronicznej podpisuje cyfrowo (część) cyfrowego obiektu lub zapisu, prywatny klucz podpisu tego dostawcy powinien być przechowywany i używany w kwalifikowanym urządzeniu do składania kwalifikowanego podpisu elektronicznego lub kwalifikowanej pieczęci elektronicznej albo w bezpiecznym urządzeniu kryptograficznym, które jest wiarygodnym systemem certyfikowanym zgodnie z:

a) wspólnymi kryteriami oceny bezpieczeństwa technologii informacyjnych, określonymi w normie ISO/IEC 15408 lub we wspólnych kryteriach oceny bezpieczeństwa technologii informacyjnych, wersja CC:2022, części 1–5, opublikowanych przez uczestników porozumienia w sprawie uznawania certyfikatów wspólnych kryteriów w dziedzinie bezpieczeństwa informatycznego i certyfikowanych zgodnie z EAL na poziomie 4 lub wyższym; lub

b) europejskim programem certyfikacji cyberbezpieczeństwa opartym na wspólnych kryteriach (rozporządzenia wykonawcze Komisji (UE) 2024/482, (UE) 2024/3144) i certyfikowanym zgodnie z EAL na poziomie 4 lub wyższym; lub

c) do dnia 31.12.2030 r. FIPS PUB 140-3 poziom 3.

— Certyfikacja ta dotyczy celu lub profilu zabezpieczeń lub projektu modułu i dokumentacji bezpieczeństwa, które spełniają wymogi niniejszego dokumentu, w oparciu o analizę ryzyka i z uwzględnieniem fizycznych i innych nietechnicznych środków bezpieczeństwa.

— Jeżeli bezpieczne urządzenie kryptograficzne korzysta z certyfikacji EUCC (rozporządzenie wykonawcze (UE) 2024/482, rozporządzenie wykonawcze Komisji (UE) 2024/3144), urządzenie to musi być skonfigurowane i używane zgodnie z tą certyfikacją.

— Dostawca usług zaufania w zakresie archiwizacji elektronicznej monitoruje siłę algorytmu kryptograficznego, który był i jest stosowany. W przypadku gdy jeden z używanych algorytmów lub parametrów zostanie uznany za nieodpowiedni zgodnie z definicją zawartą w zarządzaniu ryzykiem, dostawca usług zaufania w zakresie archiwizacji elektronicznej aktualizuje odnośną politykę archiwizacji albo tworzy nowy profil archiwizacji w celu obsługi zarchiwizowanych pakietów informacji (AIP) oraz określa i realizuje odpowiednie środki.

— Ocena algorytmów kryptograficznych i ich stosowanie przez dostawcę usług zaufania w zakresie archiwizacji elektronicznej muszą być zgodne z uzgodnionymi mechanizmami kryptograficznymi zatwierdzonymi przez Europejską Grupę ds. Certyfikacji Cyberbezpieczeństwa i opublikowanymi przez ENISA (ACM-ECCG).

— Przed nawiązaniem komunikacji elementy techniczne usług zaufania w zakresie archiwizacji elektronicznej uwierzytelniają się wzajemnie w oparciu o techniki kryptograficzne.

f) Sieć (klauzula 7.9)

— Zastosowanie mają wymogi określone w klauzuli 7.8 „Bezpieczeństwo sieci" normy ETSI EN 319 401.

— Wymagany w pkt REQ-7.8-13 normy ETSI EN 319 401 skan podatności przeprowadza się co najmniej raz na kwartał.

— Wymagany w pkt REQ-7.8-17X normy ETSI EN 319 401 test penetracyjny przeprowadza się co najmniej raz w roku.

— Zapory sieciowe należy skonfigurować tak, aby uniemożliwić wszelkie protokoły i dostępy, które nie są wymagane do funkcjonowania EATSP.

g) Gromadzenie dowodów (klauzula 7.11)

— Zastosowanie mają wymogi określone w klauzuli 7.10 „Gromadzenie dowodów" normy ETSI EN 319 401, w tym w odniesieniu do zdarzeń krytycznych i innych niż krytyczne (zob. klauzula 13.2).

h) Zakończenie działalności i plan zakończenia działalności dostawcy usług zaufania w zakresie archiwizacji elektronicznej (klauzula 7.13)

— Zastosowanie mają wymagania klauzuli 7.13 normy CEN/TS 18170.

— Plan zakończenia działalności dostawcy usług zaufania w zakresie archiwizacji elektronicznej musi spełniać wymogi określone w aktach wykonawczych przyjętych na podstawie art. 24 ust. 5 rozporządzenia (UE) nr 910/2014.

i) Wiarygodny czas zdarzeń (klauzula 13.3.1)

— Zastosowanie mają wymagania klauzuli 13.3.1 normy CEN/TS 18170.

— W przypadku stosowania znaczników czasu dostawca usług zaufania w zakresie archiwizacji elektronicznej stosuje kwalifikowany znacznik czasu.