



2026/1778

17.7.2026

ROZPORZĄDZENIE WYKONAWCZE KOMISJI (UE) 2026/1778

z dnia 16 lipca 2026 r.

**ustanawiające rozwiązania wykonawcze dotyczące rejestru cyfrowych paszportów produktów
ustanowionego rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2024/1781**

(Tekst mający znaczenie dla EOG)

KOMISJA EUROPEJSKA,

uwzględniając Traktat o funkcjonowaniu Unii Europejskiej,

uwzględniając rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/1781 z dnia 13 czerwca 2024 r. w sprawie ustanowienia ram ustalania wymogów ekoprojektu w odniesieniu do zrównoważonych produktów oraz zmiany dyrektywy (UE) 2020/1828 i rozporządzenia (UE) 2023/1542 i uchylenia dyrektywy 2009/125/WE⁽¹⁾, w szczególności jego art. 13 ust. 5 akapit drugi w związku z art. 13 ust. 5 akapit trzeci,

a także mając na uwadze, co następuje:

- (1) W art. 13 ust. 1 rozporządzenia (UE) 2024/1781 zobowiązano Komisję do stworzenia cyfrowego rejestru cyfrowych paszportów produktów („rejestr”) w celu przechowywania w bezpieczny sposób co najmniej niepowtarzalnych identyfikatorów. Konieczne jest określenie głównych komponentów rejestru oraz ról i obowiązków technicznych i operacyjnych podmiotów gospodarczych, które wprowadzają produkt do obrotu lub oddają go do użytku w ramach rejestru cyfrowych paszportów produktów, właściwych organów krajowych i organów celnych oraz Komisji. Ponadto konieczne jest ustanowienie systemu rejestracji w celu rejestrowania i monitorowania operacji i interakcji przeprowadzanych w rejestrze, aby zapewnić rozliczalność wszystkich użytkowników oraz określić odpowiedzialność za utrzymanie, obsługę i bezpieczeństwo rejestru. Te rozwiązania wykonawcze obejmują również przepisy dotyczące korzystania z rejestru, mające zastosowanie do podmiotów łańcucha wartości, właściwych organów krajowych i organów celnych oraz Komisji. W stosownych przypadkach właściwe organy krajowe powinny mieć możliwość aktualizacji lub zmiany statusu cyfrowego paszportu produktu na podstawie kontroli przeprowadzonych w ramach ich zadań określonych w odpowiednich przepisach prawa Unii i prawa krajowego zgodnego z prawem Unii.
- (2) Rejestr powinien zawierać informacje na temat produktów objętych aktami delegowanymi przyjętymi na podstawie rozporządzenia (UE) 2024/1781 w zakresie, w jakim przewidziano stosowanie cyfrowego paszportu produktu, oraz na temat baterii na podstawie rozporządzenia Parlamentu Europejskiego i Rady (UE) 2023/1542⁽²⁾. Przechowywanie informacji o produktach w rejestrze może być wymagane na mocy dalszych przepisów Unii. Jest tak już w przypadku wyrobów budowlanych objętych zakresem rozporządzenia Parlamentu Europejskiego i Rady (UE) 2024/3110⁽³⁾, zabawek objętych zakresem rozporządzenia Parlamentu Europejskiego i Rady (UE) 2025/2509⁽⁴⁾ oraz detergentów i środków powierzchniowo czynnych dla użytkownika końcowego objętych zakresem rozporządzenia Parlamentu Europejskiego i Rady (UE) 2026/405⁽⁵⁾. W przypadku gdy dalsze przepisy Unii będą odnosić się do rejestru

⁽¹⁾ Dz.U. L, 2024/1781, 28.6.2024, s. 1, ELI: <http://data.europa.eu/eli/reg/2024/1781/oj>.

⁽²⁾ Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2023/1542 z dnia 12 lipca 2023 r. w sprawie baterii i zużytych baterii, zmieniające dyrektywę 2008/98/WE i rozporządzenie (UE) 2019/1020 oraz uchylające dyrektywę 2006/66/WE (Dz.U. L 191 z 28.7.2023, s. 1, ELI: <http://data.europa.eu/eli/reg/2023/1542/oj>).

⁽³⁾ Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/3110 z dnia 27 listopada 2024 r. w sprawie ustanowienia zharmonizowanych zasad wprowadzania do obrotu wyrobów budowlanych i uchylenia rozporządzenia (UE) nr 305/2011 (Dz.U. L, 2024/3110, 18.12.2024, ELI: <http://data.europa.eu/eli/reg/2024/3110/oj>).

⁽⁴⁾ Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2025/2509 z dnia 26 listopada 2025 r. w sprawie bezpieczeństwa zabawek oraz uchylające dyrektywę 2009/48/WE (Dz.U. L, 2025/2509, 12.12.2025, ELI: <http://data.europa.eu/eli/reg/2025/2509/oj>).

⁽⁵⁾ Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2026/405 z dnia 11 lutego 2026 r. w sprawie detergentów i środków powierzchniowo czynnych oraz uchylenia rozporządzenia (WE) nr 648/2004 (Dz.U. L, 2026/405, 2.3.2026, ELI: <http://data.europa.eu/eli/reg/2026/405/oj>).

utworzonego na podstawie rozporządzenia (UE) 2024/1781, zastosowanie powinny mieć rozwiązania wykonawcze określone w niniejszym rozporządzeniu. Powinno to pozostawać bez uszczerbku dla szczegółowych przepisów unijnych dotyczących rejestru cyfrowych paszportów produktów, w tym przepisów przyjętych na podstawie uprawnień do uzupełnienia lub dostosowania wymogów, które go dotyczą, tak jak ma to miejsce w przypadku wyrobów budowlanych, jak przewidziano w art. 79 ust. 2 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2024/3110 ⁽⁶⁾. W przypadku gdy rejestr jest połączony z innymi systemami informacyjnymi, połączenie takie nie powinno zakłócać interoperacyjności tych systemów.

- (3) Aby zapewnić skuteczność, bezpieczeństwo i interoperacyjność rejestru, powinien on składać się z następujących elementów: strony internetowej zapewniającej bezpieczny interfejs użytkownika; interfejsu programowania aplikacji (API) do celów rejestracji cyfrowych paszportów produktów; platformy weryfikacyjnej służącej do weryfikacji i potwierdzania istnienia i kompletności cyfrowych paszportów produktów; systemu identyfikacji i zezwoleń dla użytkowników; schematu generowania niepowtarzalnych identyfikatorów rejestracji; komponentu pamięci do przechowywania niepowtarzalnych identyfikatorów i kodów towarów w przypadku produktów, które mają zostać objęte procedurą celną „dopuszczenie do obrotu”; repozytorium semantycznego, które służy jako autorytatywne odniesienie w zakresie znaczenia semantycznego, struktury, wersjonowania i interoperacyjności danych zawartych w cyfrowym paszporcie produktu; systemu rejestracji odpowiednich operacji. Biorąc pod uwagę, że system cyfrowych paszportów produktów opiera się na modelu zdecentralizowanym, rejestr powinien zawierać też referencyjny wykaz zweryfikowanych dostawców usług w zakresie cyfrowych paszportów produktów zarejestrowanych w rejestrze.
- (4) Aby zapewnić rozliczalność, w procesie weryfikacji należy zidentyfikować każdy podmiot gospodarczy i podmiot łańcucha wartości (np. dostawcę usług w zakresie cyfrowych paszportów produktów, podmiot zajmujący się naprawą, odnawianiem, regeneracją lub recyklingiem).
- (5) W przypadku osoby fizycznej prowadzącej jednoosobową działalność gospodarczą, która musi mieć siedzibę w Unii, tożsamość należy udowodnić za pomocą kwalifikowanego podpisu elektronicznego popartego kwalifikowanym certyfikatem podpisu elektronicznego zgodnie z rozporządzeniem Parlamentu Europejskiego i Rady (UE) nr 910/2014 ⁽⁷⁾ lub za pomocą środka identyfikacji elektronicznej, który spełnia wymogi tego rozporządzenia w zakresie wysokiego poziomu bezpieczeństwa, lub za pomocą elektronicznego poświadczenia atrybutów wydanego na podstawie prawa Unii, które umożliwia identyfikację podmiotu gospodarczego. W przypadku osoby fizycznej prowadzącej jednoosobową działalność gospodarczą, która nie musi mieć siedziby w Unii, tożsamość należy udowodnić za pomocą kwalifikowanego podpisu elektronicznego popartego kwalifikowanym certyfikatem podpisu elektronicznego zgodnie z rozporządzeniem (UE) nr 910/2014 lub za pomocą elektronicznego poświadczenia atrybutów wydanego na podstawie prawa Unii, które umożliwia identyfikację podmiotu gospodarczego.
- (6) W przypadku osoby prawnej, która musi mieć siedzibę w Unii, dowód jej tożsamości oraz dowód potwierdzający jej siedzibę powinny być weryfikowane przez kwalifikowanego dostawcę usług zaufania za pomocą kwalifikowanej pieczęci elektronicznej potwierdzonej kwalifikowanym certyfikatem pieczęci elektronicznej zgodnie z rozporządzeniem (UE) nr 910/2014 lub za pomocą kwalifikowanego elektronicznego poświadczenia atrybutów wydanego na podstawie prawa Unii, które umożliwia identyfikację tożsamości i siedziby podmiotu gospodarczego. W przypadku osoby prawnej, która nie musi mieć siedziby w Unii, dowód jej tożsamości oraz, w stosownych przypadkach, dowód potwierdzający jej siedzibę powinny być weryfikowane za pomocą kwalifikowanej pieczęci elektronicznej potwierdzonej kwalifikowanym certyfikatem pieczęci elektronicznej wydanym przez kwalifikowanego dostawcę usług zaufania na podstawie rozporządzenia (UE) nr 910/2014 lub za pomocą elektronicznego poświadczenia atrybutów wydanego na podstawie prawa Unii, które umożliwia identyfikację podmiotu gospodarczego.
- (7) Niniejsze rozporządzenie powinno pozostawać bez uszczerbku dla wymogów określonych w innych aktach prawa Unii dotyczących miejsca siedziby podmiotów gospodarczych lub, w stosownych przypadkach, podmiotów łańcucha wartości, które wprowadzają produkty do obrotu lub oddają je do użytku. W związku z tym, w przypadku gdy takie wymogi mają zastosowanie, korzystanie z rejestru nie powinno prowadzić do obchodzenia ani podważania ich stosowania, a rejestr powinien działać w sposób w pełni z nimi zgodny.

⁽⁶⁾ Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/3110 z dnia 27 listopada 2024 r. w sprawie ustanowienia zharmonizowanych zasad wprowadzania do obrotu wyrobów budowlanych i uchylenia rozporządzenia (UE) nr 305/2011 (Dz.U. L 2024/3110, ELI: <http://data.europa.eu/eli/reg/2024/3110/oj>).

⁽⁷⁾ 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 (Dz.U. L 257 z 28.8.2014, s. 73, ELI: <http://data.europa.eu/eli/reg/2014/910/oj>).

- (8) Po zakończeniu procesu weryfikacji podmiot gospodarczy należy uznać za „zweryfikowany podmiot gospodarczy”, upoważniony do tworzenia profilu użytkownika i zarządzania prawami dostępu dla dodatkowych użytkowników działających w imieniu tego samego podmiotu, do rejestrowania nowych cyfrowych paszportów produktów w rejestrze i do zmiany istniejących rejestracji. Jedynie podmiot gospodarczy posiadający status „zweryfikowany” powinien mieć możliwość rejestrowania cyfrowych paszportów produktów w rejestrze i dokonywania korekt w istniejących rejestracjach, co przyczyni się do zapewnienia integralności i dokładności danych. Wykorzystywane w ramach rejestru statusy powinny wskazywać, czy rejestracja zweryfikowanego podmiotu gospodarczego jest ważna. Jeden proces weryfikacji powinien zapewniać podmiotowi gospodarczemu status „zweryfikowany” do czasu wygaśnięcia jego środków identyfikacji elektronicznej, a w każdym razie nie dłużej niż przez trzy lata. W przypadku gdy podmiot gospodarczy nie powtórzy tego procesu po upływie trzyletniego okresu lub gdy jego środki identyfikacji wygasną, nie należy go już uznawać za „zweryfikowany podmiot gospodarczy”. W związku z tym utraci on zdolność rejestrowania nowych cyfrowych paszportów produktów lub modyfikowania danych w rejestrze.
- (9) Podmioty łańcucha wartości (podmioty zajmujące się naprawą, odnawianiem, regeneracją lub inne podmioty) zamierzające uzyskać dostęp do rejestru będą musiały przejść proces weryfikacji opisany w art. 5. W związku z tym dostęp do rejestru cyfrowych paszportów produktów mają mieć wyłącznie podmioty, które uzyskały status „zweryfikowany”. Ich rolę (np. podmiotu zajmującego się naprawą, recyklingiem, regeneracją lub innego podmiotu) oraz wszelkie czynności, które wykonują w rejestrze, należy określić w aktach delegowanych przyjętych na podstawie rozporządzenia (UE) 2024/1781 lub na podstawie innych aktów prawa Unii.
- (10) Podmioty gospodarcze lub podmioty łańcucha wartości, które nie przeszły weryfikacji tożsamości w terminie przewidzianym w niniejszym rozporządzeniu, powinny mieć możliwość przeniesienia swoich zarejestrowanych cyfrowych paszportów produktów na zweryfikowany podmiot gospodarczy lub, w stosownych przypadkach, na zweryfikowany podmiot łańcucha wartości, który ma przejąć obowiązki związane z tymi cyfrowymi paszportami produktów. Takie przeniesienie może być również możliwe w przypadku każdego zweryfikowanego podmiotu gospodarczego lub zweryfikowanego podmiotu łańcucha wartości w sytuacji zmian organizacyjnych, takich jak połączenie, podział lub sprzedaż całości lub części podmiotu, zaprzestanie działalności lub inne okoliczności.
- (11) Aby zapewnić właściwe funkcjonowanie rejestru i rozliczalność dla użytkowników, należy ustanowić przepisy dotyczące zarządzania danymi zawartymi w profilu użytkownika zweryfikowanych podmiotów gospodarczych i zweryfikowanych podmiotów łańcucha wartości. W tym celu każdy zweryfikowany podmiot gospodarczy i zweryfikowany podmiot łańcucha wartości powinien zawsze dysponować co najmniej jedną osobą powiązaną z kontem w rejestrze, która zarządza danymi w ramach profilu. Obejmuje to między innymi: przyznawanie praw dostępu dodatkowym użytkownikom, o ile jest to możliwe, modyfikowanie i przeglądanie istniejących rejestracji oraz rejestrowanie nowych cyfrowych paszportów produktów. Może to być również ta sama osoba, która rejestruje zweryfikowany podmiot gospodarczy lub zweryfikowany podmiot łańcucha wartości w rejestrze. Zweryfikowany podmiot gospodarczy i zweryfikowany podmiot łańcucha wartości powinny prowadzić dokładną, kompletną i aktualną ewidencję w rejestrze oraz zapewniać poprawność wszystkich przekazywanych informacji, w tym wszelkich zmian dotyczących ich przedstawiciela prawnego. Podmiot gospodarczy i podmioty łańcucha wartości powinny być również odpowiedzialne za zarządzanie procesem weryfikacji tożsamości elektronicznej w rejestrze. Rejestr nie powinien uniemożliwiać zgodnego z prawem przeniesienia własności rejestracji cyfrowych paszportów produktów na jakiegokolwiek inny zweryfikowany podmiot gospodarczy lub zweryfikowany podmiot łańcucha wartości, niezależnie od ich statusu weryfikacji tożsamości. W przypadku gdy rejestr cyfrowych paszportów produktów jest zintegrowany z już ustanowionymi systemami unijnymi (takimi jak europejski rejestr produktów do celów etykietowania energetycznego („EPREL")), w przypadku których stosuje się ten sam poziom weryfikacji w odniesieniu do podmiotów gospodarczych lub, w stosownych przypadkach, zweryfikowanych podmiotów łańcucha wartości, należy unikać podwójnej weryfikacji.
- (12) Właściwe organy krajowe, takie jak organy nadzoru rynku, i organy celne powinny mieć dostęp do rejestru do celów wykonywania obowiązków na podstawie przysługujących im praw dostępu określonych w odpowiednich przepisach unijnych i krajowych zgodnie z prawem Unii. Aby usprawnić zarządzanie dostępem i zapewnić rozliczalność, każde państwo członkowskie powinno wyznaczyć jednego administratora krajowego jako główny punkt kontaktowy z Komisją, który będzie zarządzał prawami dostępu dla tego państwa członkowskiego i sprawował nad nimi nadzór. Wyznaczony administrator krajowy powinien działać jako organ centralny odpowiedzialny za zarządzanie prawami dostępu dla wszystkich odpowiednich organów krajowych w danym państwie członkowskim, aby zapewnić przydzielanie praw dostępu do rejestru jedynie odpowiednim organom. Rola wyznaczonych administratorów krajowych nie obejmuje wypełniania obowiązków określonych w art. 22 w odniesieniu do danego państwa członkowskiego. Państwa członkowskie powinny poinformować Komisję o imieniu i nazwisku lub nazwie oraz danych kontaktowych wyznaczonego administratora krajowego i powiadomić Komisję o wszelkich zmianach tych informacji. Aby zapewnić bezpieczeństwo, integralność i poufność danych, przekazanie praw dostępu powinno odbywać się na pełną odpowiedzialność państwa członkowskiego, z uwzględnieniem szczególnych potrzeb jego organów.

- (13) Zarządzając rejestrem zgodnie z art. 13 ust. 1 rozporządzenia (UE) 2024/1781, Komisja powinna zagwarantować przetwarzanie danych osobowych według najwyższych standardów ochrony danych zgodnie z rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2018/1725⁽⁸⁾. Komisję należy zatem uznać za „administratora” rejestru zdefiniowanego w art. 3 pkt 8 tego rozporządzenia. Dane osobowe powinny być przetwarzane wyłącznie do celów zarządzania rejestrem i jego funkcjonowania. Informacje te należy chronić przed nieuprawnionym dostępem, wykorzystywaniem lub udostępnianiem. Dane te należy przechowywać jedynie tak długo, jak jest to konieczne, i usuwać w przypadku usunięcia kont użytkowników lub cofnięcia dostępu. Jeżeli jednak czynności wykonywane przez użytkownika w rejestrze wymagają zatrzymywania danych do celów audytu lub identyfikowalności na podstawie prawa Unii, dane te należy odpowiednio przechowywać.
- (14) Podmiot gospodarczy powinien dokonywać rejestracji cyfrowego paszportu produktu w rejestrze na poziomie szczegółowości określonym w mającym zastosowanie prawie Unii, a mianowicie na poziomie modelu, partii lub artykułu. Aby zapewnić pełną funkcjonalność rejestru, w szczególności dla właściwych organów krajowych i organów celnych, w przypadku tworzenia cyfrowego paszportu produktu na poziomie artykułu wraz z tym cyfrowym paszportem produktu należy zarejestrować w rejestrze również odpowiednie identyfikatory partii i modelu, o ile istnieje projekt partii i modelu dla danego produktu. W przypadku produktów, które ze względu na swój charakter są unikalne, w tym towarów wytwarzanych ręcznie, nie wymaga się identyfikatorów partii ani modelu. Ta sama zasada ma zastosowanie do cyfrowych paszportów produktów wydawanych na poziomie partii, w przypadku których przy rejestracji wymagany jest identyfikator modelu. W tym kontekście identyfikator partii i identyfikator modelu powinny odzwierciedlać grupę wyższego szczebla danego produktu. Identyfikatory te powinien wydawać podmiot gospodarczy, aby umożliwić właściwym organom krajowym śledzenie produktów należących do konkretnej partii lub modelu zarejestrowanych w rejestrze cyfrowych paszportów produktów. W przypadku gdy ten sam produkt podlega różnym przepisom unijnym wymagającym rejestracji jego cyfrowego paszportu produktu na różnych poziomach szczegółowości (model, partia lub artykuł), cyfrowy paszport produktu powinien być rejestrowany na najbardziej szczegółowym z tych poziomów.
- (15) Rejestracji należy dokonać za pośrednictwem bezpiecznego interfejsu użytkownika w ramach rejestru udostępnionego przez Komisję lub za pośrednictwem utworzonego w tym celu API. Po pomyślnym zatwierdzeniu rejestracji cyfrowego paszportu produktu następuje wygenerowanie niepowtarzalnego identyfikatora rejestracji i jego zapisanie w rejestrze oraz automatyczne przekazanie zgodnie z art. 8 podmiotowi rejestrującemu cyfrowy paszport produktu za pośrednictwem tej samej usługi, z której podmiot ten skorzystał w celu przesłania danych cyfrowego paszportu produktu.
- (16) W celu zagwarantowania, aby rejestrowano wyłącznie kompletne i ważne cyfrowe paszporty produktów, Komisja, jako właściciel rejestru i podmiot nim zarządzający zgodnie z art. 13 ust. 1 rozporządzenia (UE) 2024/1781, powinna przeprowadzać automatyczną weryfikację przedkładanych danych. Powinna ona obejmować co najmniej weryfikację struktury danych i poziomu szczegółowości (model, partia lub artykuł) cyfrowego paszportu produktu dla tego odnośnego produktu zgodnie z mającymi zastosowanie przepisami unijnymi. W stosownych przypadkach weryfikacji powinny podlegać również kody towarów i link do kopii zapasowej przechowywanej przez dostawcę usług w zakresie cyfrowych paszportów produktów. Weryfikacja poprawności merytorycznej zarejestrowanych danych pozostaje zadaniem organów nadzoru rynku zgodnie z mającymi zastosowanie przepisami unijnymi. W związku z tym automatycznych weryfikacji nie należy uznawać za dowód zgodności z wymogami zawartymi w przepisach unijnych mających zastosowanie do produktu, w tym z przepisami dotyczącymi nadzoru rynku.
- (17) W przypadku gdy cyfrowy paszport produktu jest zarejestrowany w rejestrze, podmiot gospodarczy lub, w stosownych przypadkach, osoba trzecia działająca w imieniu podmiotu gospodarczego jest uprawniona do wystąpienia do rejestru o dowód rejestracji. Wniosek ten może obejmować co najmniej jeden cyfrowy paszport produktu, za który podmiot gospodarczy jest odpowiedzialny. Dowód rejestracji powinien służyć jako dowód dla osób trzecich na to, że dany cyfrowy paszport produktu został prawidłowo zarejestrowany. Powinien on zostać utworzony jako bezpieczny dokument elektroniczny, który można pobrać z rejestru. Dowód ten powinien pozostać dostępny przez 90 dni kalendarzowych od daty wygenerowania, z możliwością ponownego utworzenia w razie potrzeby.

⁽⁸⁾ 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>).

- (18) Aby zapewnić poprawność i dokładność danych zawartych w rejestrze, rejestr powinien obsługiwać wersjonowanie zarejestrowanych danych. Każda nowa wersja cyfrowego paszportu produktu powinna być powiązana z pierwotnym identyfikatorem rejestracji, a każda aktualizacja powinna być opatrzona znacznikiem czasu. Do celów bezpiecznego przetwarzania danych w rejestrze należy również rejestrować wszystkie przeprowadzone operacje. W przypadkach gdy prawo Unii nie określa, jak długo cyfrowy paszport produktu musi pozostawać dostępny, dane rejestracyjne cyfrowego paszportu produktu zostaną automatycznie usunięte z rejestru po upływie 10 lat od rejestracji zgodnie z zasadami określonymi w zawiadomieniu Komisji „Niebieski przewodnik – wdrażanie unijnych przepisów dotyczących produktów 2022”⁽⁹⁾. W przypadku gdy prawo Unii określa konkretny okres przechowywania, dane będą przechowywane w rejestrze przez ten konkretny okres.
- (19) Aby zapewnić interoperacyjność semantyczną cyfrowych paszportów produktów i techniczne funkcjonowanie rejestru, należy utworzyć repozytorium semantyczne. Repozytorium semantyczne będzie ewoluującym zbiorem modeli danych i definicji semantycznych, stopniowo rozszerzanym w miarę włączania dodatkowych grup produktów. Wszystkie dane zawarte w cyfrowym paszporcie produktu muszą być ustrukturyzowane zgodnie ze wspólnymi modelami danych i definicjami semantycznymi opublikowanymi w repozytorium semantycznym rejestru. Ramy te powinny zachować elastyczność i możliwość rozszerzenia, aby można było uwzględnić wszelkie przyszłe zmiany wymogów dotyczących danych związanych z włączeniem produktu do cyfrowego paszportu produktu. Komisja dąży do zapewnienia, aby repozytorium semantyczne posiadało możliwości techniczne pozwalające na publikowanie specyfikacji semantycznych i ich wymianę z innymi repozytoriami na szczeblu Unii, w tym z repozytoriami prowadzonymi przez instytucje i organy Unii.
- (20) Aby umożliwić przeglądanie, wyszukiwanie i porównywanie definicji semantycznych i struktur danych, repozytorium semantyczne powinno obejmować usługę wyszukiwania. Komisja powinna zapewnić, aby zawartość repozytorium semantycznego była zawsze dostępna za pośrednictwem publicznie udokumentowanych API, z wyjątkiem okresów niezbędnych działań w zakresie utrzymania lub tymczasowego zawieszenia usług zgodnie z art. 15. API powinny obsługiwać wspólne formaty danych, aby ułatwić ich automatyczne wykorzystywanie przez systemy zewnętrzne. Dostęp do repozytorium semantycznego i jego API oraz korzystanie z nich powinny być bezpłatne.
- (21) Komisja powinna ustanowić usługę pomocy technicznej, aby w razie potrzeby zapewnić odpowiednie wsparcie techniczne wszystkim użytkownikom rejestru. Usługa pomocy technicznej powinna być dostępna przez cały rok w standardowych godzinach pracy. Dalsze informacje szczegółowe, w tym procedury operacyjne, należy udostępnić na stronie internetowej Komisji.
- (22) Aby zapewnić integralność, bezpieczeństwo i przejrzystość rejestru, Komisja powinna prowadzić solidny i zautomatyzowany system rejestracji wszystkich działań w ramach rejestru. W ramach systemu rejestracji należy stworzyć kompleksowe ścieżki audytu. W tym celu oraz w celu śledzenia wszystkich czynności wykonywanych w rejestrze, aby zapewnić rozliczalność dla wszystkich użytkowników, należy rejestrować próby dostępu, zarówno udane, jak i nieudane, a także modyfikacje i czynności administracyjne.
- (23) Okresy przechowywania logów powinny być proporcjonalne do ich celów. Chociaż logi dotyczące modyfikacji danych powinny być przechowywane przez czas trwania rejestracji w celu wsparcia długoterminowej weryfikacji, dochodzeń w sprawie incydentów i przestrzegania obowiązków prawnych, w przypadku logów prób uwierzytelnienia wymaga się krótszego okresu przechowywania, aby zrównoważyć potrzeby w zakresie bezpieczeństwa z zasadami minimalizacji danych. Logi operacji administracyjnych i wymiany danych są przechowywane średnio przez okres pięciu lat.
- (24) Dostęp właściwych organów krajowych i organów celnych do logów w celu prowadzenia dochodzeń lub audytów bezpieczeństwa lub w przypadku incydentów ma zasadnicze znaczenie dla skutecznej współpracy i egzekwowania przepisów. Takiego dostępu należy udzielać w sposób zapewniający poufność i integralność logów, a jednocześnie umożliwiając terminowe i skrupulatne dochodzenia lub audyty.

⁽⁹⁾ Zawiadomienie Komisji „Niebieski przewodnik – wdrażanie unijnych przepisów dotyczących produktów 2022” (Tekst mający znaczenie dla EOG) 2022/C 247/01 (Dz.U. C 247 z 29.6.2022, s. 1).

- (25) Biorąc pod uwagę wrażliwy charakter rejestrowanych danych, które mogą obejmować dane osobowe lub informacje poufne, Komisja powinna wdrożyć odpowiednie środki techniczne i organizacyjne w celu ochrony logów przed nieuprawnionym dostępem lub niezgodnym z prawem przetwarzaniem, przypadkową utratą, zniszczeniem lub uszkodzeniem. Takie środki powinny gwarantować ciągłość i poufność logów, a także zapewniać ich integralność i wiarygodność jako dowodów. Stosowanie szyfrowania, kontroli dostępu i regularnych kontroli integralności należy uznać za najlepsze praktyki w zakresie wypełniania tych obowiązków.
- (26) Aby ułatwić skuteczne i efektywne korzystanie z rejestru, Komisja powinna zapewnić jasne, dostępne i aktualne wytyczne, a także instrukcje dotyczące procedur rejestracji i zarządzania danymi. Udostępnienie tych zasobów za pośrednictwem strony internetowej Komisji zagwarantuje, że wszyscy użytkownicy, niezależnie od posiadanej technicznej wiedzy fachowej, będą w stanie wywiązać się z obowiązków. Takie wytyczne mają zasadnicze znaczenie dla zminimalizowania błędów, zmniejszenia obciążeń administracyjnych i promowania jednolitego stosowania wymogów dotyczących rejestracji w całej Unii.
- (27) Stała dostępność rejestru jest podstawowym wymogiem jego właściwego funkcjonowania, ponieważ przerwy mogą zakłócić działania związane z zapewnieniem zgodności, nadzór rynku, kontrole celne oraz swobodny przepływ towarów i usług na rynku wewnętrznym. Planowane działania w zakresie utrzymania, takie jak aktualizacje oprogramowania, poprawki zabezpieczeń lub aktualizacje systemu, mogą jednak czasami wymagać tymczasowej niedostępności. Aby złagodzić zakłócenia, Komisja powinna z wyprzedzeniem informować o takich okresach na publicznie dostępnej stronie internetowej, co umożliwi użytkownikom odpowiednie planowanie. Ponadto w wyjątkowych okolicznościach, takich jak nieprawidłowe działanie systemu, cyberataki lub nagłe zagrożenia bezpieczeństwa, Komisja może zawiesić dostęp do rejestru bez uprzedzenia, aby zapobiec naruszeniom ochrony danych, nieuprawnionemu dostępowi lub dalszym szkodom. Takie środki są uzasadnione nadrzędną potrzebą ochrony integralności i bezpieczeństwa rejestru i zawartych w nim danych. W przypadku takiego zawieszenia dostępu Komisja powinna podjąć szybkie działania w celu przywrócenia normalnego funkcjonowania oraz, w miarę możliwości, jak najszybciej poinformować użytkowników o zawieszeniu i przewidywanym czasie jego trwania. Aby zapewnić rozliczalność i umożliwić dostęp organom nadzoru rynku i organom celnym, Komisja powinna dokumentować czas trwania i harmonogram wszelkich wyłączeń oraz przechowywać taką ewidencję przez co najmniej pięć lat.
- (28) Rejestr powinien działać zgodnie z wysokimi standardami bezpieczeństwa w celu ochrony integralności, poufności i dostępności zawartych w nim danych. W związku z tym Komisja powinna przygotować plan bezpieczeństwa informatycznego obejmujący ocenę ryzyka związanego z cyberbezpieczeństwem i innymi kwestiami informatycznymi, przeprowadzać audyty techniczne oraz kontrole wyrywkowe w celu weryfikacji zgodności i identyfikacji podatności, aby zapewnić odporność systemu na cyberzagrożenia. Komisja powinna dopilnować, aby wszystkie zdarzenia związane z bezpieczeństwem, które obejmują między innymi nieuprawniony dostęp, nieuprawnione przetwarzanie, naruszenia ochrony danych, błędy w logice wdrażania, rejestrowano zgodnie ze standardami bezpieczeństwa technologii informacyjnych stosowanymi przez Komisję. Ponadto rejestr powinien być zgodny – gdy tylko odpowiednie usługi będą dostępne na rynku unijnym – z odpowiednim poziomem suwerenności, w oparciu o ramy suwerenności chmurowej ⁽¹⁰⁾.
- (29) Komisja powinna mieć możliwość wdrożenia niezbędnych środków w przypadku podejrzenia oszukańczych czynności w rejestrze, które mogą obejmować niewłaściwe pobieranie informacji. W przypadku podejrzenia szkodliwego działania użytkownicy mają obowiązek niezwłocznego powiadomienia Komisji oraz, w stosownych przypadkach, organów krajowych, których to dotyczy.
- (30) Przetwarzanie danych osobowych w rejestrze jest konieczne zgodnie z rozporządzeniem (UE) 2024/1781 i obejmuje weryfikację cyfrowych paszportów produktów, nadzór rynku i kontrole celne. Aby zapewnić autentyczność i integralność danych oraz chronić prawa osób, których dane dotyczą, przechowywane w rejestrze dane osobowe, takie jak imiona i nazwiska, dane kontaktowe i dane uwierzytelniające, powinny być przetwarzane zgodnie z rozporządzeniem (UE) 2018/1725.

⁽¹⁰⁾ Ramy suwerenności chmurowej (https://commission.europa.eu/document/09579818-64a6-4dd5-9577-446ab6219113_en).

- (31) Podmiot gospodarczy powinien być odpowiedzialny za przekazanie do rejestru dokładnych i kompletnych informacji. Biorąc pod uwagę potencjalne ryzyko związane z nieuprawnionym dostępem do rejestru, takie jak modyfikacja danych, podmiot gospodarczy powinien być zobowiązany do wdrożenia odpowiednich technicznych i organizacyjnych środków bezpieczeństwa w celu ochrony swoich systemów informatycznych, w szczególności danych uwierzytelniających wykorzystywanych do uzyskiwania dostępu do rejestru. Podmiot gospodarczy powinien ponosić odpowiedzialność nawet wtedy, gdy do rejestracji cyfrowego paszportu produktu w jego imieniu upoważniona jest osoba trzecia.
- (32) Komisja, która ma być właścicielem rejestru i podmiotem nim zarządzającym, powinna być odpowiedzialna za ogólne zarządzanie cyklem życia rejestru, w tym za jego opracowanie, dostępność, monitorowanie, aktualizację, utrzymanie i hosting. Czynności te wiążą się między innymi z dostępem Komisji do rejestru. Komisja powinna mieć również możliwość dostępu do rejestru w celu uzyskania informacji niezbędnych do realizacji działań wymaganych na mocy innych aktów ustawodawczych UE, w tym do celów nadzoru rynku, ochrony konsumentów i przestrzegania przepisów prawa celnego.
- (33) Komisja powinna też nadal być odpowiedzialna za zapewnienie, aby przechowywane w nim dane były przetwarzane w sposób bezpieczny i zgodny z prawem Unii, w tym z przepisami w zakresie ochrony danych.
- (34) Państwa członkowskie muszą mieć możliwość interakcji z rejestrem w celu skutecznego prowadzenia nadzoru rynku, kontroli celnych i innych zadań określonych na szczeblu krajowym lub w prawie Unii. Państwa członkowskie powinny pozostać odpowiedzialne za zapewnienie opracowania, utrzymania i bezpieczeństwa krajowych komponentów, z których korzystają w celu uzyskiwania dostępu do systemu, takich jak krajowe rejestry lub systemy informacyjne. Aby zagwarantować odpowiednią ochronę danych osobowych zgodnie z rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679⁽¹⁾, państwa członkowskie należy uznawać za administratorów w rozumieniu art. 4 pkt 7 tego rozporządzenia, gdy przetwarzają dane osobowe w celach określonych w prawie Unii. Państwa członkowskie są uprawnione do przetwarzania danych uzyskanych z rejestru zgodnie z prawem Unii.
- (35) Środki przewidziane w niniejszym rozporządzeniu są zgodne z opinią komitetu ustanowionego na mocy art. 73 rozporządzenia (UE) 2024/1781,

PRZYJMUJE NINIEJSZE ROZPORZĄDZENIE:

Artykuł 1

Przedmiot i zakres stosowania

1. W niniejszym rozporządzeniu określa się rozwiązania wykonawcze dotyczące funkcjonowania rejestru cyfrowych paszportów produktów ustanowionego zgodnie z art. 13 rozporządzenia (UE) 2024/1781, w tym przepisy mające zastosowanie do podmiotów gospodarczych, które wprowadzają do obrotu lub oddają do użytku którykolwiek z następujących produktów wymagających istnienia cyfrowego paszportu produktu i jego rejestracji w rejestrze:
- a) produkty objęte aktami delegowanymi przyjętymi na podstawie art. 4 rozporządzenia (UE) 2024/1781;
 - b) baterie objęte art. 77 rozporządzenia (UE) 2023/1542;
 - c) wyroby budowlane objęte art. 76 rozporządzenia (UE) 2024/3110;
 - d) zabawki objęte art. 19 rozporządzenia (UE) 2025/2509;
 - e) detergenty i środki powierzchniowo czynne dla użytkownika końcowego objęte art. 21 rozporządzenia (UE) 2026/405;
 - f) każdy inny produkt objęty przepisami Unii wymagający cyfrowego paszportu produktu i jego rejestracji w rejestrze ustanowionym na podstawie art. 13 rozporządzenia (UE) 2024/1781.

⁽¹⁾ 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>).

2. Te rozwiązania wykonawcze obejmują również przepisy regulujące korzystanie z rejestru przez podmioty łańcucha wartości, właściwe organy krajowe, organy celne i Komisję. Rozwiązania wykonawcze i przepisy, o których mowa w ust. 1 niniejszego artykułu, odnoszą się do:

- a) zarządzania dostępem do rejestru;
- b) procesu weryfikacji umożliwiającego weryfikację podmiotów gospodarczych i podmiotów łańcucha wartości;
- c) technicznej konfiguracji rejestru, w tym repozytorium semantycznego, oraz systemu rejestracji związanego z modelami wymiany danych i zarządzaniem wersjami oprogramowania;
- d) procesu rejestracji i przechowywania niepowtarzalnych identyfikatorów;
- e) procesu rejestracji i przechowywania kodów towarów dla produktów, które mają zostać objęte procedurą celną „dopuszczenie do obrotu”;
- f) wymogów dotyczących rejestracji – w stosownych przypadkach – poziomu szczegółowości cyfrowego paszportu produktu: modelu, partii, artykułu;
- g) statusów związanych z danymi zawartymi w zarejestrowanych cyfrowych paszportach produktów;
- h) danych, które umożliwią identyfikowalność produktów w ramach ich odpowiedniej grupy produktów, na wszystkich poziomach szczegółowości, o których mowa w art. 8 ust. 2, mających zastosowanie do ich cyfrowego paszportu produktu;
- i) aktualizacji i usuwania danych rejestracyjnych;
- j) przetwarzania danych osobowych;
- k) środków mających na celu zapobieganie wszelkim przypadkom niewłaściwego lub oszukańczego korzystania z rejestru, wykrywanie takich przypadków i reagowanie na nie;
- l) audytów technicznych;
- m) zapewnienia dostępności rejestru i zawartych w nim danych.

Artykuł 2

Definicje

Do celów niniejszego rozporządzenia stosuje się następujące definicje:

- 1) „rejestr cyfrowych paszportów produktów” lub „rejestr” oznacza system informacyjny ustanowiony i utrzymywany przez Komisję zgodnie z art. 13 rozporządzenia (UE) 2024/1781;
- 2) „dane uwierzytelniające” oznaczają zbiór niepowtarzalnych identyfikatorów, takich jak nazwa użytkownika i hasło, które umożliwiają użytkownikowi weryfikację swojej tożsamości w celu jej uwierzytelnienia w rejestrze;
- 3) „token uwierzytelniający” oznacza token, który służy do przekazywania w bezpieczny sposób informacji o skutecznym uwierzytelnieniu, wykorzystywany do potwierdzania uwierzytelnionych sesji lub dostępu delegowanego między aplikacjami a systemem informacyjnym cyfrowego paszportu produktu;
- 4) „proces weryfikacji tożsamości” oznacza proces, w ramach którego osoba fizyczna lub prawna przedstawia dowód tożsamości oraz, w stosownych przypadkach, dowód potwierdzający siedzibę;
- 5) „zweryfikowany podmiot gospodarczy” oznacza podmiot gospodarczy, który pomyślnie zakończył proces weryfikacji tożsamości w rejestrze zgodnie z art. 4;
- 6) „podmiot łańcucha wartości” oznacza osobę fizyczną lub prawną inną niż podmiot gospodarczy, która prowadzi działalność w łańcuchu wartości produktu wymagającego cyfrowego paszportu produktu i jego rejestracji w rejestrze, taką jak podmiot zajmujący się naprawą, odnawianiem, regeneracją lub recyklingiem;
- 7) „zweryfikowany podmiot łańcucha wartości” oznacza podmiot łańcucha wartości, który pomyślnie przeszedł proces weryfikacji tożsamości w rejestrze zgodnie z art. 5;

- 8) „repozytorium semantyczne” oznacza zbiór modeli danych i definicji semantycznych, które składają się z uporządkowanego i logicznie powiązanego zestawu pojęć i ich znaczeń określających podstawowe elementy cyfrowego paszportu produktu, definicje nazw lub słowników, elementy danych i ontologię związaną z konkretnymi danymi w celu zapewnienia wspólnego zrozumienia przez wszystkich użytkowników oraz interpretacji wielojęzycznej stosowanej do walidacji cyfrowego paszportu produktu i łączenia danych zawartych w rejestrze z cyfrowymi paszportami produktów;
- 9) „interoperacyjność semantyczna” oznacza zdolność systemów informacyjnych i obsługujących je organizacji do wymiany danych w taki sposób, aby znaczenie wymienianych informacji było wzajemnie zrozumiałe i jednoznacznie interpretowane przez wszystkie strony, niezależnie od stosowanej technologii lub jurysdykcji;
- 10) „słownik kontrolowany” oznacza uporządkowany i autorytatywny zestaw znormalizowanych pojęć o określonych znaczeniach służący zapewnieniu spójnego przedstawienia atrybutów danych w cyfrowych paszportach produktów;
- 11) „specyfikacja semantyczna” oznacza każdy artefakt opublikowany w repozytorium semantycznym, w tym ontologie, modele danych, słowniki kontrolowane i listy kodowe, wraz z metadanymi dotyczącymi ich wersjonowania i informacjami o pochodzeniu;
- 12) „zgodność semantyczna” oznacza zakres, w jakim dane zawarte w cyfrowym paszporcie produktu są zgodne z mającą zastosowanie specyfikacją semantyczną, przy czym:
 - a) obecne są wszystkie elementy danych wymagane aktami delegowanymi przyjętymi na podstawie art. 4 rozporządzenia (UE) 2024/1781 lub innymi przepisami prawa Unii;
 - b) obowiązkowe (wymagane i określone) i opcjonalne (niewymagane, ale określone) elementy danych zdefiniowane w aktach delegowanych przyjętych na podstawie art. 4 rozporządzenia (UE) 2024/1781 lub w innych przepisach prawa Unii są zgodne z mającymi zastosowanie wymogami, takimi jak wymogi dotyczące struktury, formatu, rodzaju wartości, słownika kontrolowanego i zasad stosowania oraz
 - c) te elementy danych mogą być interpretowane spójnie przez inne systemy przez odniesienie do mającego zastosowanie repozytorium semantycznego;
- 13) „model danych” oznacza ustrukturyzowane ramy, które służą do organizacji elementów danych, standaryzacji struktury, określenia, w jaki sposób są one ze sobą powiązane, oraz identyfikacji podmiotów, ich atrybutów i relacji między tymi podmiotami;
- 14) „system rejestracji” oznacza zautomatyzowany system, w którym rejestruje się i przechowuje informacje na temat wszystkich operacji i interakcji przeprowadzonych w rejestrze;
- 15) „model wymiany danych” oznacza ustrukturyzowane ramy, za pomocą których można wymieniać dane między różnymi systemami i platformami;
- 16) „skrót wersji cyfrowego paszportu produktu” oznacza wynik wygenerowany na podstawie odpowiednich danych elektronicznych przy użyciu algorytmu kryptograficznego z odpowiedniej wersji cyfrowego paszportu produktu;
- 17) „masowe pobieranie danych” oznacza pobieranie wyjątkowo dużego lub złożonego zbioru danych – zazwyczaj w skali sięgającej od terabajtów po petabajty – który przekracza możliwości przetwarzania lub przechowywania przez konwencjonalne narzędzia lub pojedynczą lokalną maszynę lub zakłóca działanie zabezpieczeń w zakresie monitorowania.

Stosuje się definicje „produktu”, „grupy produktów”, „cyfrowego paszportu produktu”, „dostawcy usług w zakresie cyfrowych paszportów produktów”, „wprowadzenia do obrotu”, „oddania do użytku”, „podmiotu gospodarczego” określone odpowiednio w art. 2 pkt 1, 5, 28, 32, 40, 41 i 46 rozporządzenia (UE) 2024/1781.

Do celów niniejszego rozporządzenia „cyfrowy paszport produktu” obejmuje paszport baterii ustanowiony w art. 77 rozporządzenia (UE) 2023/1542.

Stosuje się definicje „uwierzytelniania”, „kwalifikowanego podpisu elektronicznego”, „kwalifikowanego dostawcy usług zaufania”, „kwalifikowanej pieczęci elektronicznej”, „kwalifikowanego certyfikatu pieczęci elektronicznej” i „elektronicznego znacznika czasu” określone odpowiednio w art. 3 pkt 5, 12, 20, 27, 30 i 33 rozporządzenia (UE) nr 910/2014.

Stosuje się definicję „formatu nadającego się do odczytu maszynowego” określoną w art. 2 pkt 13 dyrektywy Parlamentu Europejskiego i Rady (UE) 2019/1024 ⁽¹²⁾.

Stosuje się definicję „przetwarzania” określoną w art. 3 pkt 3 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2018/1725 ⁽¹³⁾.

Stosuje się definicję „incydentu” określoną w art. 6 pkt 6 dyrektywy Parlamentu Europejskiego i Rady (UE) 2022/2555 ⁽¹⁴⁾.

Stosuje się definicję „administratora” określoną w art. 3 pkt 8 rozporządzenia (UE) 2018/1725.

Stosuje się definicje „nadzoru rynku”, „organu nadzoru rynku” i „dopuszczenia do obrotu” określone odpowiednio w art. 3 pkt 3, 4 i 25 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2019/1020 ⁽¹⁵⁾.

Stosuje się definicje „organów celnych” i „kontrol celnych” zawarte odpowiednio w art. 5 pkt 1 i 3 rozporządzenia (WE) nr 952/2013.

Artykuł 3

Struktura rejestru

Rejestr składa się z następujących elementów:

- a) strony internetowej zapewniającej bezpieczny interfejs użytkownika umożliwiający dostęp do rejestru podmiotom gospodarczym, podmiotom łańcucha wartości, właściwym organom krajowym i organom celnym;
- b) API na potrzeby rejestracji cyfrowego paszportu produktu i otrzymywania informacji z rejestru;
- c) platformy weryfikacyjnej służącej do potwierdzania i weryfikacji istnienia i kompletności cyfrowych paszportów produktów;
- d) systemu generowania niepowtarzalnych identyfikatorów rejestracji;
- e) komponentu pamięci do przechowywania co najmniej niepowtarzalnych identyfikatorów i kodów towarów dla produktów, które mają zostać objęte procedurą celną „dopuszczenie do obrotu”;
- f) wykazu zweryfikowanych dostawców usług w zakresie cyfrowych paszportów produktów zarejestrowanych w rejestrze;
- g) repozytorium semantycznego;
- h) systemu rejestracji;
- i) systemów identyfikacji i zezwoleń dla użytkowników rejestru.

⁽¹²⁾ Dyrektywa Parlamentu Europejskiego i Rady (UE) 2019/1024 z dnia 20 czerwca 2019 r. w sprawie otwartych danych i ponownego wykorzystywania informacji sektora publicznego (wersja przekształcona) (Dz.U. L 172 z 26.6.2019, s. 56, ELI: <http://data.europa.eu/eli/dir/2019/1024/oj>).

⁽¹³⁾ 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 (Tekst mający znaczenie dla EOG) (Dz.U. L 295 z 21.11.2018, ELI: <http://data.europa.eu/eli/reg/2018/1725/oj>).

⁽¹⁴⁾ 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>).

⁽¹⁵⁾ Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/1020 z dnia 20 czerwca 2019 r. w sprawie nadzoru rynku i zgodności produktów oraz zmieniające dyrektywę 2004/42/WE oraz rozporządzenia (WE) nr 765/2008 i (UE) nr 305/2011 (Dz.U. L 169 z 25.6.2019, s. 1, ELI: <http://data.europa.eu/eli/reg/2019/1020/oj>).

Artykuł 4

Wymogi w zakresie weryfikacji dotyczące podmiotów gospodarczych

1. Podmioty gospodarcze będące osobami fizycznymi prowadzącymi jednoosobową działalność gospodarczą uznaje się za „zweryfikowane podmioty gospodarcze”, jeżeli spełnią jeden z następujących warunków:
 - a) w przypadku gdy muszą mieć siedzibę w Unii – przedstawia dowód tożsamości za pomocą kwalifikowanego podpisu elektronicznego popartego kwalifikowanym certyfikatem podpisu elektronicznego zgodnie z rozporządzeniem (UE) nr 910/2014; lub przedstawia dowód tożsamości za pomocą środka identyfikacji elektronicznej, który spełnia wymogi rozporządzenia (UE) nr 910/2014 dotyczące „wysokiego” poziomu bezpieczeństwa, lub za pomocą elektronicznego poświadczenia atrybutów wydanego na podstawie prawa Unii, które umożliwia identyfikację podmiotu gospodarczego;
 - b) w przypadku gdy nie muszą mieć siedziby w Unii – przedstawia dowód tożsamości za pomocą kwalifikowanego podpisu elektronicznego popartego kwalifikowanym certyfikatem podpisów elektronicznych zgodnie z rozporządzeniem (UE) nr 910/2014 lub za pomocą elektronicznego poświadczenia atrybutów wydanego na podstawie prawa Unii, które umożliwia identyfikację podmiotu gospodarczego.
2. Podmioty gospodarcze działające jako osoby prawne uznaje się za „zweryfikowane podmioty gospodarcze”, jeżeli spełnią jeden z następujących warunków:
 - a) w przypadku gdy muszą mieć siedzibę w Unii – przedstawia dowód tożsamości i dowód potwierdzający siedzibę za pomocą kwalifikowanej pieczęci elektronicznej potwierdzonej kwalifikowanym certyfikatem pieczęci elektronicznej wydanym przez kwalifikowanego dostawcę usług zaufania zgodnie z rozporządzeniem (UE) nr 910/2014; lub, po przedstawieniu dowodu tożsamości i dowodu potwierdzającego siedzibę, za pomocą kwalifikowanego elektronicznego poświadczenia atrybutów wydanego na podstawie prawa Unii, które umożliwia identyfikację podmiotu gospodarczego;
 - b) w przypadku gdy nie muszą mieć siedziby w Unii – przedstawia dowód tożsamości i, w stosownych przypadkach, dowód potwierdzający siedzibę za pomocą kwalifikowanej pieczęci elektronicznej potwierdzonej kwalifikowanym certyfikatem pieczęci elektronicznej wydanym przez kwalifikowanego dostawcę usług zaufania zgodnie z rozporządzeniem (UE) nr 910/2014, lub za pomocą elektronicznego poświadczenia atrybutów wydanego na podstawie prawa Unii, które umożliwia identyfikację podmiotu gospodarczego.
3. Bez uszczerbku dla innych przepisów prawa Unii dostęp do rejestru cyfrowych paszportów produktów przyznaje się zweryfikowanym podmiotom gospodarczym do celów rejestracji cyfrowych paszportów produktów.
4. Podmioty gospodarcze zachowują status zweryfikowanych podmiotów gospodarczych do czasu wygaśnięcia ich środków identyfikacji elektronicznej, ale nie dłużej niż przez trzy lata od daty weryfikacji zgodnie z ust. 1 lub 2. Po wygaśnięciu takich środków lub upływie trzyletniego okresu, w zależności od tego, co nastąpi wcześniej, podmioty gospodarcze nie mogą już rejestrować nowych cyfrowych paszportów produktów w rejestrze ani modyfikować danych, o których mowa w art. 8. Mogą to zrobić tylko wtedy, gdy pomyślnie powtórzą proces weryfikacji tożsamości zgodnie z ust. 1 lub 2. Status cyfrowego paszportu produktu w rejestrze jest odpowiednio aktualizowany.
5. Bez uszczerbku dla ust. 4 w przypadku gdy rejestr cyfrowych paszportów produktów jest zintegrowany z innym unijnym systemem informacyjnym, w którym stosowany jest równoważny lub identyczny proces weryfikacji tożsamości, podmiot gospodarczy już zarejestrowany w tym systemie informacyjnym nie musi poddawać się nowemu procesowi weryfikacji tożsamości w rejestrze cyfrowych paszportów produktów.

Artykuł 5

Wymogi w zakresie weryfikacji dotyczące podmiotów łańcucha wartości

1. Podmiot łańcucha wartości będący osobą fizyczną prowadzącą jednoosobową działalność gospodarczą uzyskuje status zweryfikowanego podmiotu w rejestrze, jeżeli spełni jeden z dwóch następujących warunków:
 - a) w przypadku gdy musi mieć siedzibę w Unii – przedstawi dowód tożsamości za pomocą kwalifikowanego podpisu elektronicznego popartego kwalifikowanym certyfikatem podpisu elektronicznego zgodnie z rozporządzeniem (UE) nr 910/2014; lub przedstawi dowód tożsamości za pomocą środka identyfikacji elektronicznej, który spełnia wymogi rozporządzenia (UE) nr 910/2014 dotyczące „wysokiego” poziomu bezpieczeństwa, lub za pomocą elektronicznego poświadczenia atrybutów wydanego na podstawie prawa Unii, które umożliwia identyfikację podmiotu łańcucha wartości;
 - b) w przypadku gdy nie musi mieć siedziby w Unii – przedstawi dowód tożsamości za pomocą kwalifikowanego podpisu elektronicznego popartego kwalifikowanym certyfikatem podpisu elektronicznego zgodnie z rozporządzeniem (UE) nr 910/2014 lub za pomocą elektronicznego poświadczenia atrybutów wydanego na podstawie prawa Unii, które umożliwia identyfikację podmiotu łańcucha wartości.
2. Podmiot łańcucha wartości działający jako osoba prawna uzyskuje status zweryfikowanego podmiotu w rejestrze, jeżeli spełni jeden z następujących warunków:
 - a) w przypadku gdy musi mieć siedzibę w Unii – przedstawi dowód tożsamości i dowód potwierdzający siedzibę za pomocą kwalifikowanej pieczęci elektronicznej potwierdzonej kwalifikowanym certyfikatem pieczęci elektronicznej wydanym przez kwalifikowanego dostawcę usług zaufania zgodnie z rozporządzeniem (UE) nr 910/2014; lub przedstawi dowód tożsamości i dowód potwierdzający siedzibę za pomocą kwalifikowanego elektronicznego poświadczenia atrybutów wydanego na podstawie prawa Unii, które umożliwia identyfikację podmiotu łańcucha wartości;
 - b) w przypadku gdy nie musi mieć siedziby w Unii – przedstawi dowód tożsamości i, w stosownych przypadkach, dowód potwierdzający siedzibę za pomocą kwalifikowanej pieczęci elektronicznej potwierdzonej kwalifikowanym certyfikatem pieczęci elektronicznej wydanym przez kwalifikowanego dostawcę usług zaufania zgodnie z rozporządzeniem (UE) nr 910/2014, lub za pomocą elektronicznego poświadczenia atrybutów wydanego na podstawie prawa Unii, które umożliwia identyfikację podmiotu łańcucha wartości.
3. Dostęp do rejestru mają wyłącznie zweryfikowane podmioty łańcucha wartości, które mogą wykonywać czynności w rejestrze, jeżeli jest to określone w odpowiednich przepisach prawa Unii.
4. Podmiot łańcucha wartości zachowuje status podmiotu zweryfikowanego do czasu wygaśnięcia jego środków identyfikacji elektronicznej, a w każdym razie nie dłużej niż przez trzy lata od daty weryfikacji zgodnie z ust. 1 lub 2. Po wygaśnięciu takich środków lub po upływie trzyletniego okresu, w zależności od tego, co nastąpi wcześniej, podmioty te nie mogą już dokonywać rejestracji ani modyfikować żadnych danych w rejestrze. Mogą to zrobić tylko wtedy, gdy pomyślnie powtórzą proces weryfikacji tożsamości zgodnie z ust. 1 lub 2.
5. Bez uszczerbku dla ust. 4 w przypadku gdy rejestr cyfrowych paszportów produktów jest zintegrowany z innym unijnym systemem informacyjnym, w którym stosowany jest równoważny lub identyczny proces weryfikacji tożsamości, podmiot łańcucha wartości już zarejestrowany w tym systemie informacyjnym nie musi poddawać się nowemu procesowi weryfikacji tożsamości w rejestrze cyfrowych paszportów produktów.

Artykuł 6

Zarządzanie profilem użytkownika zweryfikowanego podmiotu gospodarczego i zweryfikowanego podmiotu łańcucha wartości

1. W przypadkach przewidzianych w prawie Unii zweryfikowane podmioty gospodarcze i zweryfikowane podmioty łańcucha wartości mogą przekazać prawa dostępu użytkownikom zewnętrznym działającym w ich imieniu.
2. Wszelkie dane osobowe wprowadzane do profilu użytkownika zweryfikowanego podmiotu gospodarczego lub zweryfikowanego podmiotu łańcucha wartości przetwarza się zgodnie z rozporządzeniem (UE) 2018/1725.

3. Poszczególne podmioty gospodarcze i poszczególne podmioty łańcucha wartości są odpowiedzialne za zarządzanie swoim procesem weryfikacji elektronicznej zgodnie z odpowiednio art. 4 i 5.
4. Zweryfikowany podmiot gospodarczy i zweryfikowany podmiot łańcucha wartości są odpowiedzialne za zapewnienie aktualizacji danych na swój temat w przypadku jakiegokolwiek istotnej zmiany.

Artykuł 6^a

Przenoszenie zarejestrowanych cyfrowych paszportów produktów

Zarejestrowane cyfrowe paszporty produktów można przenieść na inny zweryfikowany podmiot gospodarczy lub, w stosownych przypadkach, na zweryfikowany podmiot łańcucha wartości, który przejmie obowiązki poprzedniego podmiotu w odniesieniu do tych cyfrowych paszportów produktów od wskazanej daty przeniesienia.

Artykuł 7

Organy krajowe

1. Najpóźniej do dnia 18 lutego 2027 r. państwa członkowskie wyznaczają administratora krajowego, który będzie pełnił funkcję pojedynczego oficjalnego punktu kontaktowego dla Komisji do celów zarządzania prawami dostępu do rejestru dla tego państwa członkowskiego.
2. Państwa członkowskie przekazują Komisji imię i nazwisko lub nazwę oraz dane kontaktowe wyznaczonego administratora krajowego oraz powiadamiają Komisję o wszelkich późniejszych zmianach dotyczących wyznaczonego administratora krajowego.
3. Wyznaczony administrator krajowy może przekazać prawa dostępu do rejestru odpowiednim organom krajowym w swoim państwie członkowskim. Takie przekazanie odbywa się na pełną odpowiedzialność państwa członkowskiego i w sposób zapewniający bezpieczeństwo, integralność i poufność danych zawartych w rejestrze, do których uzyskano dostęp zgodnie z niniejszym rozporządzeniem.
4. Organy krajowe, którym wyznaczony administrator krajowy przyznał dostęp, mogą dalej przekazywać prawa dostępu do rejestru i zarządzać nimi w ramach swoich odpowiednich uprawnień.
5. Dane osobowe zawarte w profilach użytkowników i na kontach użytkowników właściwych organów krajowych i organów celnych są przetwarzane przez Komisję jako administratora zgodnie z rozporządzeniem (UE) 2018/1725.

Artykuł 8

Rejestracja cyfrowego paszportu produktu

1. W przypadku produktów, o których mowa w art. 1 ust. 1 lit. a), cyfrowy paszport produktu jest rejestrowany przez zweryfikowany podmiot gospodarczy wprowadzający produkt do obrotu lub oddający go do użytku na poziomie określonym w mających zastosowanie aktach delegowanych (poziom modelu, partii lub artykułu) przyjętych na podstawie art. 4 rozporządzenia (UE) 2024/1781.
2. W przypadku produktów, o których mowa w art. 1 ust. 1 lit. b)–f), cyfrowy paszport produktu jest rejestrowany przez odpowiedni podmiot na poziomie (poziom modelu, partii lub artykułu) określonym w odpowiednich przepisach prawa Unii.

W przypadku gdy prawo Unii przewiduje, że osoba trzecia wykonuje czynności w rejestrze w imieniu podmiotów, o których mowa w akapicie pierwszym lub drugim, taka osoba trzecia, po przejściu weryfikacji zgodnie z art. 19 ust. 4, będzie mogła wykonywać czynności rejestracyjne w rejestrze.

3. W przypadku gdy ten sam produkt podlega różnym przepisom unijnym wymagającym rejestracji jego cyfrowego paszportu produktu na różnych poziomach szczegółowości, cyfrowy paszport produktu rejestruje się na najbardziej szczegółowym poziomie wymaganym w odpowiednich przepisach unijnych.

4. W przypadku tworzenia cyfrowego paszportu produktu na poziomie artykułu zgodnie z ust. 1 zarówno identyfikatory partii, jak i modelu są powiązane z tym cyfrowym paszportem produktu, jeżeli dla danego produktu istnieje projekt partii i modelu.
5. W przypadku tworzenia cyfrowego paszportu produktu na poziomie partii zgodnie z ust. 1 identyfikator modelu jest powiązany z tym cyfrowym paszportem produktu, jeżeli dla danego produktu istnieje projekt modelu.
6. Odpowiedni podmiot, o którym mowa w ust. 1, rejestruje cyfrowy paszport produktu za pośrednictwem bezpiecznego interfejsu użytkownika rejestru, jak przewidziano w art. 3 lit. a), albo za pośrednictwem API, jak przewidziano w art. 3 lit. b).
7. Po złożeniu wniosku o rejestrację Komisja odczytuje treść cyfrowego paszportu produktu i automatycznie potwierdza:
 - a) zgodność semantyczną danych zawartych w cyfrowym paszporcie produktu, jak przewidziano w mających zastosowanie aktach delegowanych przyjętych na podstawie art. 4 rozporządzenia (UE) 2024/1781 lub w mających zastosowanie aktach delegowanych przyjętych na podstawie art. 77 rozporządzenia (UE) 2023/1542 lub na podstawie innych przepisów prawa Unii przewidujących rejestrację danych dotyczących cyfrowego paszportu produktu w rejestrze cyfrowych paszportów produktów;
 - b) w stosownych przypadkach – spójność obowiązkowych danych, które mają zostać wprowadzone do rejestru, z wartościami danych zawartych w cyfrowym paszporcie produktu;
 - c) zgodność cyfrowego paszportu produktu z poziomem szczegółowości (model, partia lub artykuł) przewidzianym w mających zastosowanie aktach delegowanych przyjętych na podstawie art. 4 rozporządzenia (UE) 2024/1781, w mających zastosowanie aktach delegowanych przyjętych na podstawie art. 77 rozporządzenia (UE) 2023/1542 lub w innych przepisach prawa Unii przewidujących określony poziom szczegółowości w odniesieniu do cyfrowego paszportu produktu, który ma być zarejestrowany w rejestrze;
 - d) w stosownych przypadkach – ważność kodu towaru produktu w odniesieniu do dozwolonych zakresów dla tej grupy produktów;
 - e) w stosownych przypadkach – link do kopii zapasowej przechowywanej przez dostawcę usług w zakresie cyfrowych paszportów produktów.
8. Po pomyślnej weryfikacji zgodnie z ust. 6 w rejestrze jest generowany i zapisywany niepowtarzalny i trwały identyfikator rejestracji jako część danych rejestracyjnych.
9. Ponadto Komisja przechowuje w rejestrze następujące informacje jako część danych rejestracyjnych:
 - a) w stosownych przypadkach – niepowtarzalne identyfikatory;
 - b) w stosownych przypadkach – kod towaru dla produktu;
 - c) w stosownych przypadkach – odniesienie do dostawcy usług w zakresie cyfrowych paszportów produktów;
 - d) informacje dotyczące rejestrującego, w tym daty i godziny rejestracji, oraz integralności cyfrowego paszportu produktu jako część dowodów potwierdzających dokonanie rejestracji.
10. Po pomyślnym przekazaniu danych do rejestru przez odpowiedni podmiot, o którym mowa w ust. 1, Komisja automatycznie przekazuje temu odpowiedniemu podmiotowi niepowtarzalny identyfikator rejestracji dla tego konkretnego produktu wygenerowany zgodnie z ust. 9. Niepowtarzalny identyfikator rejestracji przekazuje się za pośrednictwem interfejsu użytkownika lub odpowiedzi z API, w zależności od usługi wykorzystywanej przez odpowiedni podmiot podczas rejestracji.

Artykuł 9

Dowód rejestracji

1. Podmioty gospodarcze lub, w stosownych przypadkach, osoby trzecie w imieniu podmiotu gospodarczego, które zarejestrowały cyfrowy paszport produktu w rejestrze zgodnie z art. 8, muszą być w stanie wygenerować w dowolnym momencie dowód rejestracji w odniesieniu do co najmniej jednego cyfrowego paszportu produktu, za który te podmioty gospodarcze są odpowiedzialne.

2. Dowód rejestracji stanowi dowód, w tym względem osób trzecich, potwierdzający spełnienie obowiązku rejestracji tego cyfrowego paszportu produktu. Jest on generowany jako bezpieczny dokument elektroniczny, możliwy do pobrania z rejestru przez podmiot, który zarejestrował cyfrowy paszport produktu, i zawiera co najmniej następujące dane:

- a) niepowtarzalny identyfikator produktu;
- b) w stosownych przypadkach – kod towaru, o którym mowa w art. 8 ust. 9 lit. b);
- c) imię i nazwisko lub nazwę oraz tożsamość zweryfikowanego podmiotu gospodarczego odpowiedzialnego za rejestrację, o którym mowa w art. 8 ust. 9 lit. d);
- d) datę i godzinę rejestracji najnowszej wersji cyfrowego paszportu produktu, w odniesieniu do której wygenerowano dowód zgodnie z art. 8 ust. 9 lit. d), potwierdzonej elektronicznym znacznikiem czasu Komisji;
- e) skrót wersji cyfrowego paszportu produktu, której dotyczy wygenerowany dowód.

3. Dowód rejestracji jest gwarantowany kwalifikowaną pieczęcią elektroniczną, jak przewidziano w art. 38 rozporządzenia (UE) nr 910/2014, i zawiera elektroniczny znacznik czasu Komisji, o którym mowa w ust. 2 lit. d).

4. Komisja udostępnia w rejestrze wnioskującemu zweryfikowanemu podmiotowi gospodarczemu dowód rejestracji za pośrednictwem bezpiecznego interfejsu użytkownika rejestru lub API, w zależności od usługi wybranej przez podmiot gospodarczy. Dowód ten pozostaje dostępny przez okres 90 dni kalendarzowych od daty jego wygenerowania.

Artykuł 10

Zarządzanie danymi rejestracyjnymi

1. Wszelkie zmiany danych rejestracyjnych cyfrowego paszportu produktu, w tym ich utworzenie, modyfikacja i usunięcie, są zapisywane w systemie rejestracji rejestru zgodnie z art. 14 i odzwierciedlone w statusie rejestracji.
2. Rejestr obsługuje wersjonowanie zarejestrowanych danych oraz przechowuje się w nim znacznik czasu Komisji dla każdej aktualizacji.
3. W przypadku gdy prawo Unii nie przewiduje konkretnego okresu dostępności cyfrowego paszportu produktu, dane rejestracyjne cyfrowego paszportu produktu, o których mowa w art. 8 ust. 7 i 8, automatycznie usuwa się z rejestru po upływie 10 lat od rejestracji. W przypadku gdy prawo Unii przewiduje konkretny okres dostępności cyfrowego paszportu produktu, okres zatrzymywania takich danych dostosowuje się do okresu dostępności cyfrowego paszportu produktu.
4. Użytkownicy rejestru mają prawo zażądać usunięcia swojego konta, jeżeli nie są już odpowiedzialni za działania związane z rejestrem.

Artykuł 11

Modele danych

1. Model danych mający zastosowanie do poszczególnych grup produktów opiera się na aktach delegowanych przyjętych na podstawie art. 4 rozporządzenia (UE) 2024/1781 – o ile istnieją – lub na innych mających zastosowanie przepisach prawa Unii.
2. W stosownych przypadkach modele danych mogą opierać się na istniejących unijnych zasobach semantycznych, słownikach kontrolowanych i referencyjnych modelach danych.
3. Wszystkie dane zawarte w cyfrowym paszporcie produktu są ustrukturyzowane zgodnie ze wspólnymi modelami danych i definicjami semantycznymi publikowanymi w repozytorium semantycznym, o którym mowa w art. 12.
4. Modele danych są wersjonowane.

Artykuł 12

Repozytorium semantyczne

1. Komisja ustanawia i utrzymuje cyfrowe repozytorium semantyczne paszportów produktów, które służy jako autorytatywne i nadające się do odczytu maszynowego źródło dla modeli danych, definicji semantycznych i słowników mających zastosowanie do cyfrowych paszportów produktów we wszystkich grupach produktów. Repozytorium semantyczne należy opracować i utrzymywać zgodnie z rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2024/903 ⁽¹⁶⁾.
2. Repozytorium semantyczne zawiera co najmniej następujące elementy:
 - a) semantyczne znaczenie atrybutów danych wymaganych w cyfrowym paszporcie produktu i specyfikacjach technicznych w celu stworzenia, w stosownych przypadkach, typowanych i rozstrzygalnych powiązań między różnymi cyfrowymi paszportami produktów oraz powiązań między atrybutami cyfrowego paszportu produktu a odpowiednimi dowodami przekazywanymi w ramach łańcucha wartości produktu;
 - b) modele danych dla różnych produktów objętych zakresem niniejszego rozporządzenia i ich formaty;
 - c) zgromadzone metadane dotyczące modeli danych dla produktów;
 - d) znaczenie semantyczne ról przewidzianych w mających zastosowanie aktach delegowanych przyjętych na podstawie art. 4 rozporządzenia (UE) 2024/1781 lub w innych przepisach Unii mających zastosowanie do każdego produktu, w przypadku którego wymagane jest stosowanie cyfrowego paszportu produktu;
 - e) wielojęzyczne etykiety i definicje dla wszystkich obowiązkowych atrybutów danych.
3. Metadane, o których mowa w ust. 2 lit. c), muszą być zgodne ze specyfikacjami DCAT-AP ⁽¹⁷⁾.
4. Komisja zapewnia, aby w repozytorium semantycznym publikowano wielojęzyczne etykiety i definicje, o których mowa w ust. 2 lit. e), w odniesieniu do wszelkich atrybutów modelu danych nowo wprowadzonych do tego repozytorium.
5. Repozytorium semantyczne obejmuje usługę wyszukiwania umożliwiającą każdemu użytkownikowi przeglądanie, wyszukiwanie i pobieranie definicji semantycznych i struktur danych.
6. Komisja zapewnia, aby zawartość repozytorium semantycznego była dostępna za pośrednictwem publicznie udokumentowanych API. Te API obsługują wspólne formaty danych i zapewniają zasoby semantyczne nadające się do odczytu maszynowego, aby ułatwić ich zautomatyzowane wykorzystywanie przez systemy zewnętrzne.
7. Dostęp do repozytorium semantycznego i jego API oraz korzystanie z nich są bezpłatne.

Artykuł 13

Wsparcie techniczne

1. Komisja zapewnia usługę pomocy technicznej, aby podmioty gospodarcze, podmioty łańcucha wartości, właściwe organy krajowe oraz organy celne mogły, na wniosek, uzyskać wsparcie techniczne. Usługa pomocy technicznej jest dostępna przez cały rok w godz. 8:00–20:00 czasu obowiązującego w Brukseli. Dalsze szczegółowe informacje dotyczące jej funkcjonowania są opublikowane na stronie internetowej Komisji. Ponadto do lutego 2029 r. Komisja opracuje zautomatyzowane narzędzie wsparcia technicznego, które będzie dostępne 24 godziny na dobę przez cały rok.
2. Pisemną wymianę informacji między podmiotami gospodarczymi, podmiotami łańcucha wartości, właściwymi organami krajowymi lub organami celnymi oraz usługą pomocy technicznej przechowuje się przez sześć miesięcy po zamknięciu wniosku o wsparcie techniczne, o którym mowa w ust. 1, i udostępnia organom nadzoru rynku na żądanie.

⁽¹⁶⁾ Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/903 z dnia 13 marca 2024 r. w sprawie ustanowienia środków na rzecz wysokiego poziomu interoperacyjności sektora publicznego na terytorium Unii (Dz.U. L, 2024/903, 22.3.2024, ELI: <http://data.europa.eu/eli/reg/2024/903/oj>).

⁽¹⁷⁾ Profil aplikacji katalogu danych (<https://interoperable-europe.ec.europa.eu/collection/semic-support-centre/solution/dcat-application-profile-data-portals-europe>).

Artykuł 14

System rejestracji

1. Komisja ustanawia, utrzymuje i prowadzi system rejestracji. Komisja zapewnia utworzenie kompletnej, dokładnej i wiarygodnej ścieżki audytu w systemie rejestracji.
2. W systemie rejestracji Komisja rejestruje zdarzenia związane ze wszystkimi następującymi kategoriami czynności:
 - a) dane związane z wpisami dotyczącymi dostępu i uwierzytelnienia;
 - b) modyfikacje danych przez wszystkich użytkowników rejestru, w tym wprowadzanie lub aktualizowanie danych, o których mowa w art. 13 ust. 4 rozporządzenia (UE) 2024/1781, lub danych, które należy wprowadzić do rejestru na podstawie innych przepisów Unii nakładających obowiązek stosowania cyfrowego paszportu produktu w odniesieniu do danego produktu;
 - c) czynności administracyjne wszystkich użytkowników rejestru, w tym tworzenie, zmiana lub usuwanie kont użytkowników, zmiany praw dostępu i uprawnień oraz wszelkie zmiany konfiguracji rejestru i inne czynności administracyjne użytkowników rejestru;
 - d) logi wymiany danych.
3. Aby zapewnić bezpieczne i zgodne z prawem Unii przetwarzanie danych przechowywanych w rejestrze, Komisja utrzymuje logi przez okres:
 - a) sześciu miesięcy w przypadku kategorii czynności, o których mowa w ust. 2 lit. a);
 - b) pięciu lat w przypadku kategorii czynności, o których mowa w ust. 2 lit. c) i d);
 - c) odpowiadający czasowi trwania rejestracji zdarzeń związanych z kategoriami czynności, o których mowa w ust. 2 lit. b).
4. W przypadku podejrzenia incydentów oraz do celów audytów i kontroli wyrywkowych bezpieczeństwa przeprowadzanych przez właściwe organy krajowe i organy celne Komisja udostępnia odpowiednim organom krajowym odpowiednie logi, o których mowa w ust. 2.
5. Komisja wdraża odpowiednie środki techniczne i organizacyjne w celu zagwarantowania bezpieczeństwa wszystkich logów i ochrony ich integralności, w szczególności przed niedozwoloną lub niezgodną z prawem przetwarzaniem, przypadkową utratą, zniszczeniem lub uszkodzeniem. Środki takie zapewniają co najmniej niezmienną i poufność logów.

Artykuł 15

Utrzymanie i dostępność rejestru

1. Komisja udostępnia na swojej stronie internetowej wytyczne i instrukcje dotyczące sposobu rejestrowania danych w rejestrze i zarządzania nimi.
2. Rejestr jest dostępny przez cały czas, z wyjątkiem okresów przeprowadzania niezbędnych działań w zakresie utrzymania, takich jak wdrażanie nowych wersji oprogramowania, i bez uszczerbku dla ust. 3. W takich przypadkach Komisja z wyprzedzeniem powiadamia o niedostępności na ogólnodostępnej stronie internetowej rejestru.
3. Komisja może zawiesić dostępność rejestru bez uprzedniego powiadomienia, jeżeli jest to konieczne ze względu na awarię, cyberatak lub pilną potrzebę w zakresie bezpieczeństwa, do czasu rozwiązania problemu.
4. W przypadku gdy rejestracja jest niemożliwa ze względu na tymczasową niedostępność lub nieprawidłowe działanie rejestru, Komisja rejestruje datę i godzinę niedostępności i udostępnia takie informacje podmiotom gospodarczym, podmiotom łańcucha wartości, właściwym organom krajowym i organom celnym na ich wniosek przez okres nie krótszy niż pięć lat.

*Artykuł 16***Bezpieczeństwo systemów informacyjnych i audyty techniczne**

1. Komisja zapewnia bezpieczeństwo rejestru i jego komponentów, o których mowa w art. 3. W tym celu Komisja może przeprowadzać audyty techniczne i kontrole wrywkowe komponentów rejestru.
2. Do celów ust. 1 Komisja podejmuje niezbędne działania w celu:
 - a) uniemożliwienia nieupoważnionego dostępu do rejestru;
 - b) zapobiegania nieuprawnionemu przetwarzaniu danych zawartych w rejestrze;
 - c) wykrycia wszelkich nieuprawnionych działań w ramach rejestru;
 - d) zapobiegania wszelkim naruszeniom ochrony danych w rejestrze;
 - e) zapewnienia rejestracji zdarzeń związanych z bezpieczeństwem zgodnie ze standardami bezpieczeństwa technologii informacyjnych stosowanymi przez Komisję.

*Artykuł 17***Niewłaściwe lub oszukańcze korzystanie z rejestru**

W przypadku gdy Komisja stwierdzi niewłaściwe lub oszukańcze działanie w ramach rejestru, w tym każde takie działanie związane z masowym pobieraniem danych, wdraża niezbędne środki, aby zapobiec temu działaniu i przeciwdziałać mu oraz łagodzić jego skutki.

Każdy użytkownik, który zauważy szkodliwe działanie w ramach rejestru lub szkodliwe działanie na jego niekorzyść, lub ma uzasadnione podstawy, by podejrzewać takie działanie, niezwłocznie informuje Komisję i – w stosownych przypadkach – zainteresowane państwa członkowskie.

*Artykuł 18***Dane osobowe**

1. Komisja przechowuje w rejestrze następujące dane osobowe w celu zapewnienia weryfikacji tożsamości wszystkich użytkowników:
 - a) imię i nazwisko każdego użytkownika; lub, w stosownych przypadkach, imię i nazwisko osoby prawnie upoważnionej do działania w charakterze przedstawiciela prawnego podmiotu gospodarczego;
 - b) dane uwierzytelniające związane z użytkownikiem, w tym dane uwierzytelniające lub tokeny uwierzytelniające, niezbędne do uzyskania bezpiecznego dostępu do rejestru;
 - c) adres pocztowy podmiotów gospodarczych i podmiotów łańcucha wartości będących użytkownikami;
 - d) adres e-mail każdego użytkownika;
 - e) metadane zawarte w przesłanych dokumentach, jeżeli takie metadane przyczyniają się do identyfikacji lub weryfikacji użytkownika.
2. W przypadku osób fizycznych wymagane jest również przechowywanie identyfikatorów osobistych, takich jak numer paszportu, numer krajowego dowodu tożsamości lub numer krajowego dokumentu tożsamości elektronicznej, numer w rejestrze stanu cywilnego, numer identyfikacji podatkowej wydany przez odpowiedni organ krajowy danego państwa członkowskiego lub dowolny identyfikator państwa trzeciego przypisany osobie lub dowolny dokument identyfikujący tę osobę.
3. Zgromadzone dane osobowe są przetwarzane zgodnie z rozporządzeniem (UE) 2018/1725.

*Artykuł 19***Obowiązki zweryfikowanego podmiotu gospodarczego**

1. Zweryfikowany podmiot gospodarczy rejestrujący cyfrowy paszport produktu przekazuje Komisji jako podmiotowi zarządzającemu rejestrem wszystkie informacje niezbędne do rejestracji, jak przewidziano w art. 8. Zweryfikowany podmiot gospodarczy jest odpowiedzialny za dokładność i kompletność informacji przedłożonych w momencie rejestracji.
2. Zweryfikowany podmiot gospodarczy zapewnia, aby informacje przechowywane w rejestrze cyfrowych paszportów produktów były zawsze dokładne, kompletne i aktualne.
3. Zweryfikowany podmiot gospodarczy jest odpowiedzialny za wdrożenie odpowiednich technicznych i organizacyjnych środków bezpieczeństwa w odniesieniu do swoich systemów informatycznych i danych uwierzytelniających wykorzystywanych do uzyskania dostępu do rejestru, aby zapobiec nieuprawnionemu dostępowi do danych rejestracyjnych lub ich modyfikacji za pośrednictwem jego systemu informatycznego.
4. W przypadku gdy zweryfikowany podmiot gospodarczy upoważnia osobę trzecią do wykonywania czynności rejestracyjnych w rejestrze w jego imieniu, podmiot będący osobą trzecią musi przejść proces weryfikacji zgodnie z art. 5. Zweryfikowany podmiot gospodarczy pozostaje w pełni odpowiedzialny za wypełnianie obowiązków określonych w niniejszym rozporządzeniu.
5. Każdy zweryfikowany podmiot gospodarczy jest odpowiedzialny za dane, które przekazuje Komisji jako podmiotowi zarządzającemu rejestrem, i jest uznawany za administratora przekazywanych przez siebie danych.

*Artykuł 20***Obowiązki zweryfikowanych podmiotów łańcucha wartości**

1. W przypadku gdy zweryfikowany podmiot łańcucha wartości upoważni osobę trzecią do działania w jego imieniu, zweryfikowany podmiot łańcucha wartości pozostaje odpowiedzialny za wypełnienie obowiązków określonych w niniejszym rozporządzeniu.
2. Zweryfikowany podmiot łańcucha wartości jest odpowiedzialny za wdrożenie odpowiednich technicznych i organizacyjnych środków bezpieczeństwa w odniesieniu do swoich systemów informatycznych i danych uwierzytelniających wykorzystywanych do uzyskania dostępu do rejestru, aby zapobiec nieuprawnionemu dostępowi do danych rejestracyjnych lub ich modyfikacji za pośrednictwem jego systemu informatycznego.
3. W przypadku gdy prawo Unii przewiduje wprowadzenie jakichkolwiek informacji do rejestru cyfrowych paszportów produktów przez podmioty łańcucha wartości, każdy zweryfikowany podmiot łańcucha wartości jest odpowiedzialny za dane, które przekazuje Komisji jako podmiotowi zarządzającemu rejestrem, i jest uznawany za administratora przekazywanych przez siebie danych.

*Artykuł 21***Obowiązki Komisji**

1. Komisja zapewnia, aby dane przechowywane w rejestrze były przetwarzane w bezpieczny sposób i zgodnie z prawem Unii, w tym z mającymi zastosowanie przepisami w zakresie ochrony danych osobowych.
2. Komisja jest właścicielem rejestru i odpowiada za zarządzanie nim, w tym za jego opracowanie, dostępność, monitorowanie, aktualizację, utrzymanie i hosting.
3. Dane, które Komisja może uzyskać z rejestru, mogą być przekazywane odpowiednim służbom Komisji lub właściwym organom krajowym do celów realizacji działań wymaganych na mocy innych aktów ustawodawczych Unii, w tym nadzoru rynku, ochrony konsumentów i przestrzegania przepisów prawa celnego.

*Artykuł 22***Obowiązki państw członkowskich**

1. W przypadku gdy państwa członkowskie tworzą wzajemne połączenie z rejestrem, uznaje się je za odpowiednich właścicieli ich systemów informacyjnych, w tym wszelkich komponentów opracowanych przez państwa członkowskie na potrzeby wzajemnego połączenia. Państwa członkowskie są odpowiedzialne za ustanowienie, opracowanie, dostępność, monitorowanie, aktualizację, utrzymanie i hosting komponentów wykorzystywanych do uzyskania dostępu do rejestru, za które są odpowiedzialne.
2. Państwa członkowskie zapewniają odpowiedni poziom bezpieczeństwa krajowych komponentów wykorzystywanych do uzyskania dostępu do rejestru, zgodnie z prawem Unii. Państwa członkowskie bez zbędnej zwłoki informują Komisję o zmianach i aktualizacjach komponentów, za które są odpowiedzialne i które mogą mieć wpływ na funkcjonowanie, dostępność i niezawodność rejestru.
3. Państwa członkowskie mogą przetwarzać dane z rejestru. W przypadku gdy państwa członkowskie przetwarzają dane uzyskane z rejestru, przetwarzanie tych danych odbywa się zgodnie z prawem Unii.
4. W przypadku gdy państwa członkowskie przetwarzają dane osobowe do celów wykonywania obowiązków określonych w prawie Unii lub w prawie krajowym zgodnie z prawem Unii, uznaje się je za administratorów w rozumieniu art. 4 pkt 7 rozporządzenia (UE) 2016/679.
5. Państwa członkowskie są odpowiedzialne za wszelkie działania w zakresie przetwarzania danych prowadzone pod ich kontrolą, w tym za:
 - a) zarządzanie rejestracją i wprowadzaniem (tzw. onboarding) właściwych organów krajowych oraz, w stosownych przypadkach, organów celnych za pośrednictwem wyznaczonego krajowego administratora, o którym mowa w art. 7 ust. 2;
 - b) zapewnienie, aby wszelkie przetwarzanie danych odbywające się w ramach ich kompetencji było przeprowadzane zgodnie z rozporządzeniem (UE) 2016/679;
 - c) cofnięcie prawa dostępu użytkownika do rejestru w przypadku nieuprawnionego lub nieprawidłowego dostępu do rejestru.

*Artykuł 23***Monitorowanie i ocena**

W ramach monitorowania i oceny rozporządzenia (UE) 2024/1781 pod kątem jego wkładu w funkcjonowanie rynku wewnętrznego Komisja do końca 2032 r., a następnie co sześć lat, przeprowadza ocenę niniejszego rozporządzenia w celu uwzględnienia funkcjonowania rejestru cyfrowych paszportów produktów i w stosownych przypadkach przedstawia projekt wniosku dotyczącego jego zmiany.

*Artykuł 24***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 lipca 2026 r.

W imieniu Komisji
Przewodnicząca
Ursula VON DER LEYEN