DECYZJA WYKONAWCZA KOMISJI (UE) 2022/483

z dnia 21 marca 2022 r.

zmieniająca decyzję wykonawczą (UE) 2021/1073 ustanawiającą specyfikacje techniczne i zasady do celów wdrożenia ram zaufania unijnych cyfrowych zaświadczeń COVID ustanowionych rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2021/953

(Tekst mający znaczenie dla EOG)

KOMISJA EUROPEJSKA,

uwzględniając Traktat o funkcjonowaniu Unii Europejskiej,

uwzględniając rozporządzenie Parlamentu Europejskiego i Rady (UE) 2021/953 z dnia 14 czerwca 2021 r. w sprawie ram wydawania, weryfikowania i uznawania interoperacyjnych zaświadczeń o szczepieniu, o wyniku testu i o powrocie do zdrowia w związku z COVID-19 (unijne cyfrowe zaświadczenie COVID) w celu ułatwienia swobodnego przemieszczania się w czasie pandemii COVID-19 ([1]), w szczególności jego art. 9 ust. 1,

a także mając na uwadze, co następuje:

(1) W rozporządzeniu (UE) 2021/953 ustanowiono unijne cyfrowe zaświadczenia COVID – które stanowią dowód na to, że dana osoba otrzymała szczepionkę przeciwko COVID-19, uzyskała ujemny wynik testu lub powróciła do zdrowia po zakażeniu – w celu ułatwienia ich posiadaczom korzystania z prawa do swobodnego przemieszczania się w czasie pandemii COVID-19.

(2) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2021/954 ([2]) stanowi, że państwa członkowskie mają stosować przepisy określone w rozporządzeniu (UE) 2021/953 do obywateli państw trzecich, którzy nie są objęci zakresem stosowania tego rozporządzenia, ale którzy legalnie przebywają lub zamieszkują na ich terytorium i są uprawnieni do podróżowania do innych państw członkowskich zgodnie z prawem Unii.

(3) Zalecenie Rady (UE) 2022/290 zmieniające zalecenie (UE) 2020/912 w sprawie tymczasowego ograniczenia innych niż niezbędne podróży do UE oraz ewentualnego zniesienia takiego ograniczenia ([3]) stanowi, że obywatele państw trzecich, którzy chcą odbyć inne niż niezbędne podróże z państw trzecich do Unii, powinni posiadać ważny dowód szczepienia lub powrotu do zdrowia, taki jak unijne cyfrowe zaświadczenie COVID lub zaświadczenie COVID-19 wydane przez państwo trzecie objęte aktem wykonawczym przyjętym na podstawie art. 8 ust. 2 rozporządzenia (UE) 2021/953.

(4) Aby unijne cyfrowe zaświadczenie COVID mogło funkcjonować w całej Unii, Komisja przyjęła decyzję wykonawczą (UE) 2021/1073 ([4]), w której określono specyfikację techniczną i zasady na potrzeby wypełniania, bezpiecznego wydawania i weryfikacji unijnych cyfrowych zaświadczeń COVID, zapewnienia ochrony danych osobowych, określenia wspólnej struktury niepowtarzalnego identyfikatora zaświadczenia oraz wydawania ważnego, bezpiecznego i interoperacyjnego kodu kreskowego.

(5) Zgodnie z art. 4 rozporządzenia (UE) 2021/953 Komisja i państwa członkowskie miały ustanowić i utrzymać ramy zaufania dla unijnego cyfrowego zaświadczenia COVID. Ramy zaufania mogą wspierać dwustronną wymianę list unieważnionych certyfikatów, które to listy zawierają niepowtarzalne identyfikatory unieważnionych zaświadczeń.

([1]) Dz.U. L 211 z 15.6.2021, s. 1.

([2]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2021/954 z dnia 14 czerwca 2021 r. w sprawie ram wydawania obywatelom państw trzecich legalnie przebywającym lub zamieszkującym na terytoriach państw członkowskich w czasie pandemii COVID-19 interoperacyjnych zaświadczeń o szczepieniu, o wyniku testu i o powrocie do zdrowia w związku z COVID-19 (unijne cyfrowe zaświadczenie COVID), oraz weryfikowania i uznawania takich zaświadczeń (Dz.U. L 211 z 15.6.2021, s. 24).

([3]) Zalecenie Rady (UE) 2022/290 z dnia 22 lutego 2022 r. zmieniające zalecenie Rady (UE) 2020/912 w sprawie tymczasowego ograniczenia innych niż niezbędne podróży do UE oraz ewentualnego zniesienia takiego ograniczenia (Dz.U. L 43 z 24.2.2022, s. 79).

([4]) Decyzja wykonawcza Komisji (UE) 2021/1073 z dnia 28 czerwca 2021 r. ustanawiająca specyfikacje techniczne i zasady do celów wdrożenia ram zaufania unijnych cyfrowych zaświadczeń COVID ustanowionych rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2021/953 (Dz.U. L 230 z 30.6.2021, s. 32).

(6) 1 lipca 2021 r. uruchomiono bramę sieciową unijnych cyfrowych zaświadczeń COVID („brama sieciowa"), która jest centralnym elementem ram zaufania i umożliwia bezpieczną i godną zaufania wymianę między państwami członkowskimi kluczy publicznych wykorzystywanych do weryfikacji unijnych cyfrowych zaświadczeń COVID.

(7) Ze względu na ich pomyślne wdrożenie na dużą skalę unijne cyfrowe zaświadczenia COVID stały się celem oszustów, którzy starają się znaleźć sposoby wydawania fałszywych zaświadczeń. Te fałszywe zaświadczenia muszą zatem zostać unieważnione. Ponadto państwa członkowskie na szczeblu krajowym mogą unieważniać niektóre unijne cyfrowe zaświadczenia COVID ze względów medycznych i związanych ze zdrowiem publicznym, na przykład dlatego, że partię podanych szczepionek uznano później za wadliwą.

(8) Chociaż system unijnych cyfrowych zaświadczeń COVID jest w stanie natychmiast ujawnić przerobione zaświadczenia, nie można wykryć w innych państwach członkowskich autentycznych zaświadczeń, które zostały wydane niezgodnie z prawem na podstawie fałszywych dokumentów, nieuprawnionego dostępu lub z zamiarem oszustwa, chyba że państwa członkowskie wymienią się listami unieważnionych certyfikatów sporządzonymi na szczeblu krajowym. To samo dotyczy zaświadczeń, które unieważniono ze względów medycznych i związanych ze zdrowiem publicznym. Niewykrycie przez państwa członkowskie wniosków o weryfikację zaświadczeń unieważnionych przez inne państwa członkowskie stanowi zagrożenie dla zdrowia publicznego i podważa zaufanie obywateli do systemu unijnych cyfrowych zaświadczeń COVID.

(9) Jak zauważono w motywie 19 rozporządzenia (UE) 2021/953, ze względów medycznych oraz z powodów związanych ze zdrowiem publicznym jak również w przypadku zaświadczeń wydanych lub uzyskanych w sposób oszukańczy, państwa członkowskie powinny mieć możliwość – w ograniczonych przypadkach – ustanowienia list unieważnionych certyfikatów i ich wymiany z innymi państwami członkowskimi do celów tego rozporządzenia, w szczególności w odniesieniu do zaświadczeń, które zostały wydane w sposób błędny, w wyniku oszustwa lub w następstwie zawieszenia partii szczepionki przeciwko COVID-19 uznanej za wadliwą. Państwa członkowskie nie powinny mieć możliwości unieważnienia zaświadczeń wydawanych przez inne państwa członkowskie. Wymieniane listy unieważnionych certyfikatów nie powinny zawierać żadnych danych osobowych innych niż niepowtarzalne identyfikatory zaświadczeń. W szczególności nie powinny one zawierać powodu, dla którego unieważniono zaświadczenie.

(10) Oprócz ogólnych informacji na temat możliwości unieważnienia zaświadczeń i możliwych powodów takiego unieważnienia, odpowiedzialny organ wydający zaświadczenia powinien niezwłocznie poinformować posiadaczy unieważnionych zaświadczeń o unieważnieniu i jego powodach. Jednak w niektórych przypadkach, w szczególności w przypadku unijnych cyfrowych zaświadczeń COVID wydanych w formie papierowej, zidentyfikowanie i poinformowanie posiadacza o unieważnieniu zaświadczenia może okazać się niemożliwe lub może wymagać niewspółmiernie dużego wysiłku. Państwa członkowskie nie powinny gromadzić dodatkowych danych osobowych – niepotrzebnych w procesie wydawania – wyłącznie w celu poinformowania posiadaczy w przypadku unieważnienia ich zaświadczeń.

(11) Konieczne jest zatem wzmocnienie ram zaufania unijnych cyfrowych zaświadczeń COVID poprzez wspieranie dwustronnej wymiany list unieważnionych certyfikatów między państwami członkowskimi.

(12) Niniejsza decyzja nie obejmuje tymczasowego zawieszenia zaświadczeń w przypadkach zastosowań krajowych nieobjętych zakresem rozporządzenia w sprawie unijnego cyfrowego zaświadczenia COVID, na przykład ze względu na to, że posiadacz zaświadczenia o szczepieniu uzyskał wynik dodatni testu na SARS-CoV-2. Pozostaje to bez uszczerbku dla ustalonych procedur kontroli zasad działania w zakresie ważności zaświadczeń.

(13) Chociaż z technicznego punktu widzenia możliwe są różne architektury wymiany list unieważnionych certyfikatów, wymiana za pośrednictwem bramy sieciowej jest najbardziej odpowiednia, ponieważ ogranicza wymianę danych do już ustanowionych ram zaufania i minimalizuje zarówno liczbę możliwych punktów awarii, jak i wymiany między państwami członkowskimi w porównaniu z alternatywnym systemem peer-to-peer.

(14) W związku z tym należy wzmocnić bramę sieciową unijnych cyfrowych zaświadczeń COVID, aby wspierać bezpieczną wymianę unieważnionych unijnych cyfrowych zaświadczeń COVID do celów ich bezpiecznej weryfikacji za pośrednictwem bramy sieciowej. W tym względzie należy wdrożyć odpowiednie środki bezpieczeństwa w celu ochrony danych osobowych przetwarzanych w bramie sieciowej. Aby zapewnić wysoki poziom ochrony, państwa członkowskie powinny pseudonimizować atrybuty zaświadczenia za pomocą nieodwracalnego skrótu (ang. hash) umieszczanego na listach unieważnionych certyfikatów. W rzeczywistości niepowtarzalny identyfikator należy uznać za dane pseudonimiczne na potrzeby operacji przetwarzania przeprowadzanych w bramie.

(15) Dodatkowo należy ustanowić przepisy dotyczące roli państw członkowskich i Komisji w odniesieniu do wymiany list unieważnionych certyfikatów.

(16) Przetwarzanie danych osobowych posiadaczy zaświadczeń, za które odpowiadają państwa członkowskie, inne organizacje publiczne lub organy urzędowe w państwach członkowskich, powinno odbywać się zgodnie z rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 ([5]). Przetwarzanie danych osobowych, za które odpowiada Komisja, w celu zarządzania bramą sieciową unijnego cyfrowego zaświadczenia COVID oraz zapewnienia jej bezpieczeństwa powinno przebiegać zgodnie z rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2018/1725 ([6]).

(17) Państwa członkowskie, reprezentowane przez wyznaczone organy krajowe lub organy urzędowe, wspólnie wyznaczają cel i określają sposoby przetwarzania danych osobowych za pośrednictwem bramy sieciowej unijnego cyfrowego zaświadczenia COVID, a zatem są współadministratorami. W art. 26 rozporządzenia (UE) 2016/679 na współadministratorów prowadzących operacje przetwarzania danych osobowych nałożono wymóg określenia w przejrzysty sposób odpowiednich zakresów ich odpowiedzialności dotyczącej wypełniania obowiązków wynikających z tego rozporządzenia. W artykule tym przewidziano również, że spoczywające na współadministratorach obowiązki i ich zakres mogą być określone przez prawo Unii lub prawo państwa członkowskiego, któremu administratorzy ci podlegają. Uzgodnienie, o którym mowa w art. 26, należy włączyć do załącznika III do niniejszej decyzji.

(18) Rozporządzenie (UE) 2021/953 powierza Komisji zadanie wspierania takiej wymiany. Najwłaściwszym sposobem wypełnienia tego zadania jest zestawienie przedłożonych list unieważnionych certyfikatów w imieniu państw członkowskich. W związku z tym Komisji należy powierzyć rolę podmiotu przetwarzającego dane, aby w imieniu państw członkowskich wspierać tę wymianę przez ułatwianie wymiany list za pośrednictwem bramy sieciowej unijnych cyfrowych zaświadczeń COVID.

(19) Komisja, jako dostawca rozwiązań technicznych i organizacyjnych na potrzeby bramy sieciowej unijnych cyfrowych zaświadczeń COVID, przetwarza dane osobowe na listach unieważnionych certyfikatów w bramie sieciowej w imieniu państw członkowskich jako współadministratorów. W związku z tym Komisja pełni rolę podmiotu przetwarzającego dane. Zgodnie z art. 28 rozporządzenia (UE) 2016/679 i art. 29 rozporządzenia (UE) 2018/1725 przetwarzanie przez podmiot przetwarzający powinno odbywać się na podstawie umowy lub instrumentu prawnego, które podlegają prawu Unii lub prawu państwa członkowskiego i wiążą podmiot przetwarzający i administratora oraz określają przetwarzanie danych. Należy zatem ustanowić zasady przetwarzania danych przez Komisję w roli podmiotu przetwarzającego dane.

(20) Zadanie Komisji polegające na wsparciu nie obejmuje ustanowienia centralnej bazy danych, o której mowa w motywie 52 rozporządzenia (UE) 2021/953. Zakaz ten ma na celu uniknięcie tworzenia centralnego repozytorium wszystkich wydanych unijnych cyfrowych zaświadczeń COVID i nie uniemożliwia państwom członkowskim wymiany list unieważnionych certyfikatów, co wyraźnie przewidziano w art. 4 ust. 2 rozporządzenia (UE) 2021/953.

(21) Podczas przetwarzania danych osobowych w ramach bramy sieciowej unijnego cyfrowego zaświadczenia COVID Komisję obowiązuje decyzja Komisji (UE, Euratom) 2017/46 ([7]).

(22) Art. 3 ust. 10 rozporządzenia (UE) 2021/953 umożliwia Komisji przyjmowanie aktów wykonawczych przewidujących, że zaświadczenia COVID-19 wydane przez państwo trzecie, z którym Unia i państwa członkowskie zawarły umowę w sprawie swobodnego przemieszczania się osób umożliwiającą umawiającym się stronom ograniczenie takiego swobodnego przemieszczania się ze względu na zdrowie publiczne w sposób niedyskryminujący i niezawierającą mechanizmu włączania aktów prawnych Unii, są równoważne zaświadczeniom wydawanym zgodnie z niniejszym rozporządzeniem. Na tej podstawie w dniu 8 lipca 2021 r. Komisja przyjęła decyzję wykonawczą (UE) 2021/1126 ([8]) ustanawiającą równoważność zaświadczeń COVID-19 wydawanych przez Szwajcarię.

([5]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 (UE) 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).

([6]) 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).

([7]) Komisja publikuje dalsze informacje na temat norm bezpieczeństwa mających zastosowanie do wszystkich systemów informatycznych Komisji Europejskiej pod adresem: https://ec.europa.eu/info/publications/security-standards-applying-all-european-commission-information-systems_pl.

([8]) Decyzja wykonawcza Komisji (UE) 2021/1126 z dnia 8 lipca 2021 r. ustanawiająca równoważność zaświadczeń COVID-19 wydawanych przez Szwajcarię z zaświadczeniami wydawanymi zgodnie z rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2021/953 (Dz.U. L 243 z 9.7.2021, s. 49).

(23) Art. 8 ust. 2 rozporządzenia (UE) 2021/953 umożliwia Komisji przyjmowanie aktów wykonawczych przewidujących, że zaświadczenia COVID-19 wydawane przez państwa trzecie zgodnie z normami i systemami technologicznymi, które są interoperacyjne z ramami zaufania unijnego cyfrowego zaświadczenia COVID i umożliwiają weryfikację autentyczności, ważności i integralności zaświadczenia, a także zawierają dane określone w załączniku do rozporządzenia, mają być uznawane za równoważne unijnym cyfrowym zaświadczeniom COVID w celu ułatwienia posiadaczom korzystania z prawa do swobodnego przemieszczania się w obrębie Unii. Jak zauważono w motywie 28 rozporządzenia (UE) 2021/953, art. 8 ust. 2 tego rozporządzenia dotyczy uznawania zaświadczeń wydawanych przez państwa trzecie obywatelom Unii i członkom ich rodzin. Komisja przyjęła już kilka takich aktów wykonawczych.

(24) Aby uniknąć luk w wykrywaniu unieważnionych zaświadczeń objętych takimi aktami wykonawczymi, państwa trzecie, których zaświadczenia COVID-19 uznano za równoważne zgodnie z art. 3 ust. 10 i art. 8 ust. 2 rozporządzenia (UE) 2021/953, powinny mieć również możliwość przedkładania odpowiednich list unieważnionych certyfikatów w bramie sieciowej unijnego cyfrowego zaświadczenia COVID.

(25) Niektórzy obywatele państw trzecich, którzy posiadają unieważnione zaświadczenia COVID-19 wydane przez państwo trzecie, których zaświadczenia COVID-19 uznano za równoważne zgodnie z rozporządzeniem (UE) 2021/953, mogą nie być objęci zakresem tego rozporządzenia lub rozporządzenia (UE) 2021/954 w chwili wygenerowania przez dane państwo trzecie listy unieważnionych certyfikatów zawierającej ich zaświadczenia. W momencie wygenerowania listy unieważnionych certyfikatów przez przedmiotowe państwo trzecie nie można jednak wiedzieć, czy wszyscy obywatele państwa trzeciego posiadający unieważnione zaświadczenia są objęci zakresem stosowania któregokolwiek z rozporządzeń. Dążenie do wykluczenia osób nieobjętych zakresem stosowania któregokolwiek z tych rozporządzeń w momencie generowania list unieważnionych certyfikatów tych państw nie jest zatem wykonalne, a próba taka skutkowałaby tym, że państwa członkowskie nie byłyby w stanie wykryć unieważnionych zaświadczeń będących w posiadaniu obywateli państw trzecich podróżujących do Unii po raz pierwszy. Jednak nawet unieważnione zaświadczenia wydane tym obywatelom państw trzecich byłyby weryfikowane przez państwa członkowskie, gdy ich posiadacze podróżują do Unii, a następnie gdy podróżują po terytorium Unii. Państwa trzecie, których zaświadczenia uznano za równoważne zgodnie z rozporządzeniem (UE) 2021/953, nie uczestniczą w zarządzaniu bramą sieciową, a zatem nie są uznawane za współadministratorów.

(26) Ponadto unijne cyfrowe zaświadczenie COVID okazało się jedynym funkcjonującym na szeroką skalę i na szczeblu międzynarodowym systemem zaświadczeń COVID-19. W rezultacie unijne cyfrowe zaświadczenie COVID stało się narzędziem o rosnącym znaczeniu globalnym i przyczynia się do walki z pandemią na szczeblu międzynarodowym, bowiem ułatwia bezpieczne podróże międzynarodowe i odbudowę światowej gospodarki. W procesie przyjmowania dodatkowych aktów wykonawczych na podstawie art. 8 ust. 2 rozporządzenia (UE) 2021/953 pojawiają się nowe potrzeby dotyczące wypełniania unijnego cyfrowego zaświadczenia COVID. Zgodnie z zasadami określonymi w decyzji wykonawczej (UE) 2021/1073 pole nazwiska jest obowiązkowe w treści technicznej zaświadczenia. Konieczna jest zmiana tego wymogu w celu promowania włączenia i interoperacyjności z innymi systemami, zważywszy że w niektórych państwach trzecich istnieją osoby bez nazwiska. W przypadku gdy imię posiadacza zaświadczenia nie może zostać podzielone na dwie części, należy je umieścić w tym samym polu (nazwiska albo imienia) unijnego cyfrowego zaświadczenia COVID, jak miałoby to miejsce w przypadku dokumentu podróży lub dokumentu tożsamości posiadacza zaświadczenia. Zmiana ta pozwoliłaby również lepiej dostosować treść techniczną zaświadczeń do obecnie obowiązujących specyfikacji dotyczących dokumentów podróży nadających się do odczytu maszynowego, publikowanych przez Organizację Międzynarodowego Lotnictwa Cywilnego.

(27) Należy zatem odpowiednio zmienić decyzję wykonawczą (UE) 2021/1073.

(28) Zgodnie z art. 42 ust. 1 rozporządzenia (UE) 2018/1725 skonsultowano się z Europejskim Inspektorem Ochrony Danych, który wydał opinię dnia 11 marca 2022 r.

(29) Aby dać państwom członkowskim i Komisji wystarczająco dużo czasu na wdrożenie zmian niezbędnych do umożliwienia wymiany list unieważnionych certyfikatów za pośrednictwem bramy sieciowej unijnych cyfrowych zaświadczeń COVID, niniejsza decyzja powinna zacząć obowiązywać cztery tygodnie po jej wejściu w życie.

(30) Środki przewidziane w niniejszej decyzji są zgodne z opinią komitetu powołanego na mocy art. 14 rozporządzenia (UE) 2021/953,

PRZYJMUJE NINIEJSZĄ DECYZJĘ:

Artykuł 1

W decyzji wykonawczej (UE) 2021/1073 wprowadza się następujące zmiany:

1) dodaje się art. 5a, 5b i 5c w brzmieniu:

„*Artykuł 5a*

Wymiana list unieważnionych certyfikatów

1. Ramy zaufania unijnych cyfrowych zaświadczeń COVID umożliwiają wymianę list unieważnionych certyfikatów za pośrednictwem centralnej bramy sieciowej unijnego cyfrowego zaświadczenia COVID („brama sieciowa") zgodnie ze specyfikacjami technicznymi zawartymi w załączniku I.

2. W przypadku gdy państwa członkowskie unieważniają unijne cyfrowe zaświadczenia COVID, mogą przedłożyć listę unieważnionych certyfikatów w bramie sieciowej.

3. W przypadku gdy państwa członkowskie przedkładają listy unieważnionych certyfikatów, organy wydające prowadzą listę unieważnionych certyfikatów.

4. Jeżeli dane osobowe są wymieniane za pośrednictwem bramy sieciowej, przetwarzanie ogranicza się do celu, jakim jest wspieranie wymiany informacji o unieważnieniu. Takie dane osobowe wykorzystuje się wyłącznie do celów weryfikacji statusu unieważnienia unijnych cyfrowych zaświadczeń COVID wydanych w ramach zakresu stosowania rozporządzenia (UE) 2021/953.

5. Informacje przekazywane do bramy sieciowej obejmują następujące dane zgodnie ze specyfikacjami technicznymi określonymi w załączniku I:

a) pseudonimizowane niepowtarzalne identyfikatory unieważnionych zaświadczeń,

b) data wygaśnięcia przedłożonej listy unieważnionych certyfikatów;

6. W przypadku gdy organ wydający unieważnia unijne cyfrowe zaświadczenia COVID, które wydał na podstawie rozporządzenia (UE) 2021/953 lub rozporządzenia (UE) 2021/954 i zamierza wymieniać przedmiotowe informacje za pośrednictwem bramy sieciowej, przekazuje on do bramy sieciowej w bezpiecznym formacie informacje, o których mowa w ust. 5, w formie list unieważnionych certyfikatów, zgodnie ze specyfikacjami technicznymi określonymi w załączniku I.

7. Organy wydające zapewniają, w miarę możliwości, rozwiązanie mające na celu poinformowanie posiadaczy unieważnionych zaświadczeń – w momencie ich unieważnienia – o statusie unieważnienia ich zaświadczeń i o jego powodach.

8. Brama sieciowa gromadzi otrzymane listy unieważnień certyfikatów. Zapewnia ona narzędzia do przekazywania tych list państwom członkowskim. Automatycznie usuwa listy według terminów ich wygaśnięcia wskazanych dla poszczególnych list przedkładanych przez organ przekazujący.

9. Wyznaczone organy krajowe lub organy urzędowe państw członkowskich przetwarzające dane osobowe za pośrednictwem bramy sieciowej są współadministratorami przetwarzanych danych. Podział odpowiednich obowiązków między współadministratorami przebiega zgodnie z załącznikiem VI.

10. Komisja jest podmiotem przetwarzającym dane osobowe, które podlegają przetwarzaniu za pośrednictwem bramy sieciowej. Do kompetencji Komisji jako podmiotu przetwarzającego dane w imieniu państw członkowskich należy zapewnienie bezpieczeństwa przesyłu i przechowywania danych osobowych w ramach bramy sieciowej oraz wypełnianie obowiązków podmiotu przetwarzającego określonych w załączniku VII.

11. Skuteczność środków technicznych i organizacyjnych służących zapewnieniu bezpieczeństwa przetwarzania danych osobowych za pośrednictwem bramy sieciowej jest regularnie sprawdzana i oceniana przez Komisję i przez współadministratorów.

Artykuł 5b

Przedkładanie przez państwa trzecie list unieważnionych certyfikatów

Państwa trzecie wydające zaświadczenia COVID-19, w odniesieniu do których Komisja przyjęła akt wykonawczy na podstawie art. 3 ust. 10 lub art. 8 ust. 2 rozporządzenia (UE) 2021/953, mogą przedkładać listy unieważnionych certyfikatów COVID-19 objętych takim aktem wykonawczym do przetwarzania przez Komisję w imieniu współadministratorów za pośrednictwem bramy sieciowej, jak określono w art. 5a, zgodnie ze specyfikacjami technicznymi określonymi w załączniku I.

Artykuł 5c

Zarządzanie przetwarzaniem danych osobowych w centralnej bramie sieciowej unijnych cyfrowych zaświadczeń COVID

1. Proces decyzyjny współadministratorów jest regulowany przez grupę roboczą ustanowioną w ramach komitetu, o którym mowa w art. 14 rozporządzenia (UE) 2021/953.

2. Wyznaczone organy krajowe lub organy urzędowe państw członkowskich przetwarzające dane osobowe za pośrednictwem bramy sieciowej jako współadministratorzy wyznaczają przedstawicieli do tej grupy.";

2) w załączniku I wprowadza się zmiany zgodnie z załącznikiem I do niniejszej decyzji;

3) w załączniku V wprowadza się zmiany zgodnie z załącznikiem II do niniejszej decyzji;

4) tekst w załączniku III do niniejszej decyzji dodaje się jako załącznik VI;

5) tekst w załączniku IV do niniejszej decyzji dodaje się jako załącznik VII.

Artykuł 2

Niniejsza decyzja wchodzi w życie trzeciego dnia po jej opublikowaniu w *Dzienniku Urzędowym Unii Europejskiej*.

Niniejszą decyzję stosuje się po upływie czterech tygodni od jej wejścia w życie.

Sporządzono w Brukseli dnia 21 marca 2022 r.

W imieniu Komisji
Przewodnicząca
Ursula VON DER LEYEN

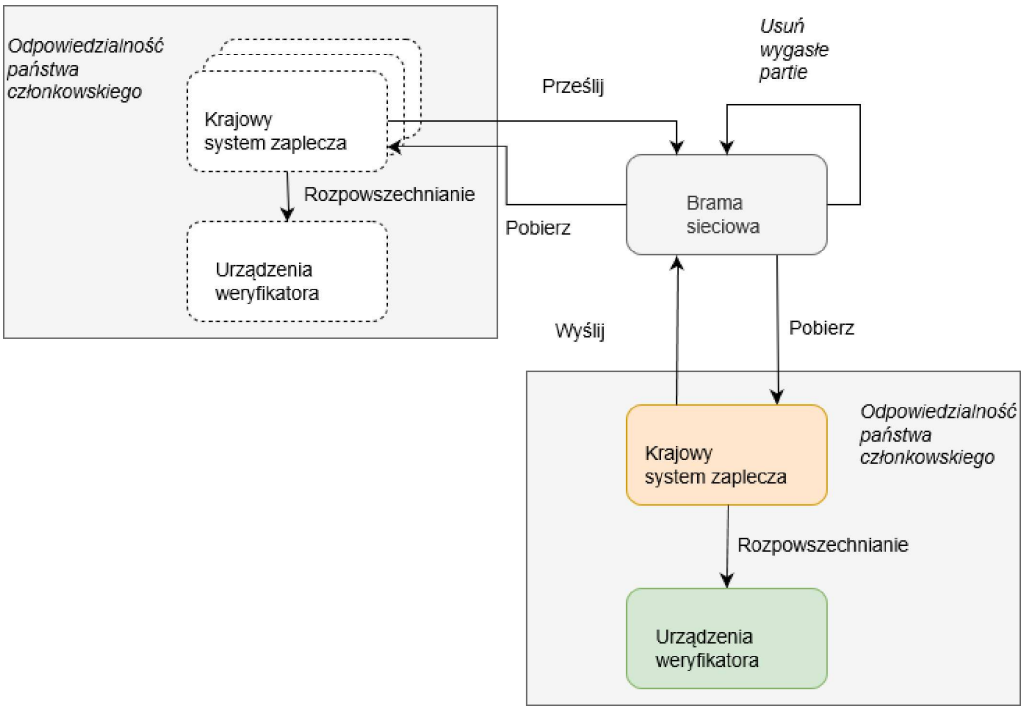
ZAŁĄCZNIK I

W załączniku I do decyzji wykonawczej (UE) 2021/1073 dodaje się sekcję 9 w brzmieniu:

„9. **ROZWIĄZANIE W ZAKRESIE UNIEWAŻNIENIA**

9.1. **Tworzenie listy unieważnionych DCC (DRL)**

Brama sieciowa zapewnia punkty końcowe i funkcje umożliwiające przechowywanie list unieważnionych certyfikatów i zarządzanie nimi:



9.2. **Model zaufania**

Wszystkie połączenia są ustanawiane na podstawie standardowego modelu zaufania DCCG w certyfikatach NB_{TLS} i NB_{UP} (zob. zarządzanie certyfikatami). Wszystkie informacje są pakowane i przesyłane za pomocą wiadomości CMS w celu zapewnienia integralności.

9.3. **Budowa partii**

9.3.1. *Partia (ang. batch)*

Każda lista unieważnionych certyfikatów zawiera jedną pozycję lub większą ich liczbę i jest pakowana w partie zawierające zestaw skrótów (ang. hashes) i ich metadanych. Partia jest niezmienna i określa datę wygaśnięcia, która wskazuje, kiedy daną partię można usunąć. Data wygaśnięcia wszystkich pozycji w partii musi być dokładnie taka sama – oznacza to, że partie muszą być pogrupowane według daty wygaśnięcia i podpisania DSC. Każda partia zawiera maksymalnie 1 000 pozycji. Jeżeli lista unieważnionych certyfikatów składa się z ponad 1 000 pozycji, wówczas tworzy się kilka partii. Każda pozycja może występować w co najwyżej jednej partii. Partia jest pakowana do struktury CMS i podpisywana certyfikatem NB_{UP} kraju wysyłającego.

9.3.2. *Indeks partii (ang. Batch Index)*

Po utworzeniu partii brama sieciowa nadaje jej niepowtarzalne ID i partia jest automatycznie dodawana do indeksu. Indeks partii jest uporządkowany według daty modyfikacji, w porządku chronologicznym rosnącym.

9.3.3. *Zachowanie bramy sieciowej*

Brama sieciowa przetwarza partie unieważnień bez żadnych zmian: nie może ona aktualizować, usuwać ani dodawać żadnych informacji do partii. Partie są przekazywane wszystkim upoważnionym krajom (zob. rozdział 9.6).

Brama sieciowa aktywnie obserwuje daty wygaśnięcia partii i usuwa partie, które wygasły. Po usunięciu partii brama sieciowa odsyła, w odniesieniu do URL usuniętej partii, komunikat „HTTP 410 Gone". W związku z tym partia pojawia się w indeksie partii jako „usunięta".

9.4. **Rodzaje skrótu (ang. Hash Types)**

Lista unieważnionych certyfikatów zawiera skróty, które mogą odpowiadać różnym rodzajom/atrybutom unieważnienia. Te rodzaje lub atrybuty są wskazane w tworzeniu list unieważnionych certyfikatów. Obecne rodzaje są następujące:

Rodzaj	Atrybut	Obliczenie skrótu (ang. Hash Calculation)
SIGNATURE	DCC Signature	SHA256 of DCC Signature
UCI	UCI (Unique Certificate Identifier)	SHA256 of UCI
COUNTRYCODEUCI	Issuing Country Code + UCI	SHA256 of Issuing CountryCode + UCI

Tylko pierwsze 128 bitów skrótów zakodowanych jako ciągi (ang. strings) base64 umieszcza się w partiach i wykorzystuje do identyfikacji unieważnionych DCC ([1]).

9.4.1. *Rodzaj skrótu: SHA256(Podpis DCC)*

W tym przypadku skrót oblicza się na podstawie bajtów podpisu COSE_SIGN1 z CWT. W przypadku podpisów RSA cały podpis zostanie wykorzystany jako dane wejściowe. Wzór dla podpisanych certyfikatów EC-DSA wykorzystuje wartość r jako dane wejściowe:

SHA256(r)

[wymagane w przypadku wszystkich nowych wdrożeń]

9.4.2. *Rodzaj skrótu: SHA256(UCI)*

W tym przypadku skrót oblicza się dla ciągu UCI zakodowanego w UTF-8 i przekształconego na tablicę bajtów (ang. byte array).

[przestarzałe ([2]), ale obsługiwane ze względu na kompatybilność wsteczną]

9.4.3. *Rodzaj skrótu: SHA256(Wydawanie CountryCode+UCI)*

W tym przypadku CountryCode zakodowano jako ciąg UTF-8 złączony z UCI zakodowanym ciągiem UTF-8. Następnie przekształca się go w tablicę bajtów i wykorzystuje jako dane wejściowe do funkcji skrótu.

[przestarzałe[2], ale obsługiwane ze względu na kompatybilność wsteczną]

9.5. **Struktura API**

9.5.1. *API dostarczająca pozycje unieważnienia*

9.5.1.1. Cel

API dostarcza pozycje listy unieważnionych certyfikatów w partiach, w tym indeks partii.

9.5.1.2. Punkty końcowe (ang. Endpoints)

([1]) W odniesieniu do szczegółowych opisów API należy również wziąć pod uwagę pkt 9.5.1.2.

([2]) Przestarzałe oznacza, że funkcja ta nie jest brana pod uwagę w przypadku nowych wdrożeń, lecz jest obsługiwana w odniesieniu do już realizowanych wdrożeń przez ściśle określony czas.

9.5.1.2.1. Punkt końcowy pobrania listy partii

Punkty końcowe są zgodne z prostym wzorem i odsyłają listę partii z małą obwolutą (ang. wrapper) dostarczającą metadane. Partie są sortowane według *daty* w porządku *rosnącym (chronologicznym)*:

/revocation-list

Verb: GET

Content-Type: application/json

Response: JSON Array

```
{
    'more':true|false,
    'batches':
        [{
            'batchId': '{uuid}',
            'country': 'XY',
            'date': '2021-11-01T00:00:00Z'
            'deleted': true | false
        }, ..
        ]
}
```

Uwaga: Wynik jest domyślnie ograniczony do 1 000. Jeżeli znacznik „more" jest ustawiony na „true", odpowiedź wskazuje, że dostępna jest większa liczba partii do pobrania. Aby pobrać więcej pozycji, klient musi ustawić nagłówek (ang. header) If-Modified-Since na datę nie wcześniejszą niż ostatni otrzymany wpis.

Odpowiedź zawiera tablicę JSON o następującej strukturze:

Pole	Definicja
more	Boolean Flag, który wskazuje, że jest więcej partii.
batches	Tablica z istniejącymi partiami.
batchId	https://en.wikipedia.org/wiki/Universally_unique_identifier
country	Kod państwa ISO 3166
date	ISO 8601 Data UTC. Data dodania lub usunięcia partii.
deleted	boolean. „True", jeżeli usunięto. Po ustawieniu znacznika „deleted" wpis może zostać ostatecznie usunięty z wyników wyszukiwania po 7 dniach.

9.5.1.2.1.1. *Kody* odpowiedzi

Kod	Opis
200	Wszystko ok.
204	Brak treści, jeżeli treść nagłówka „If-Modified-Since" nie ma odpowiednika.

Nagłówek żądania (ang. Request Header)

Nagłówek	Obowiąz-kowe	Opis
If-Modified-Since	Tak	Ten nagłówek zawiera ostatnią pobraną datę, aby uzyskać tylko najnowsze wyniki. Przy pierwszym wywołaniu nagłówek powinien być ustawiony na „2021-06-01T00:00:00Z”

9.5.1.2.2. Punkt końcowy pobrania partii

Partie zawierają wykaz identyfikatorów certyfikatu:

/revocation-list/{batchId}

Verb: GET

Accepts: application/cms

Response:CMS with Content

{

‘country’: ‘XY’,

‘expires’: ‘2022-11-01T00:00:00Z’,

‘kid’:’23S+33f=’,

‘hashType’:’SIGNATURE’,

‘entries’:[{

‘hash’:’e2e2e2e2e2e2e2e2’

}, ..]

}

Odpowiedź zawiera CMS z podpisem, który musi odpowiadać certyfikatowi NB_{UP} państwa. Wszystkie elementy na tablicy JSON mają następującą strukturę:

Pole	Obowiąz-kowe	Rodzaj	Definicja
expires	Tak	String	Data, w której element można usunąć. ISO8601 data/godzina UTC
country	Tak	String	Kod państwa ISO 3166
hashType	Tak	String	Rodzaj skrótu w podanych pozycjach (zob. rodzaje skrótów)
entries	Tak	JSON Object Array	Zob. pozycje w tabeli
kid	Tak	String	zakodowana base64 KID DSC używanego do podpisywania DCC. Jeżeli KID nie jest znany, można użyć ciągu `UNKNOWN_KID` (z wyłączeniem `).

Uwagi:

— Partie są grupowane według daty wygaśnięcia i DSC – wszystkie pozycje wygasają w tym samym czasie i zostały podpisane tym samym kluczem.

— Czas wygaśnięcia jest datą/godziną w UTC, ponieważ EU-DCC jest systemem globalnym i konieczne jest używanie jednoznacznego czasu.

— Datę wygaśnięcia trwale unieważnionego DCC ustala się na dzień wygaśnięcia odpowiedniego DSC używanego do podpisania DCC lub na czas wygaśnięcia unieważnionych DCC (w którym to przypadku stosowane godziny NumericDate/epoch traktuje się jako znajdujące się w strefie czasowej UTC).

— Krajowy system zaplecza (NB, ang. National Backend) usuwa pozycje z listy unieważnionych certyfikatów po upływie daty **wygaśnięcia**.

— NB może usunąć pozycje z listy unieważnionych certyfikatów, w przypadku gdy **kid** użyty do podpisania DCC zostanie unieważniony.

9.5.1.2.2.1. Pozycje

Pole	Obowiązkowe	Rodzaj	Definicja
hash	Tak	String	Pierwsze 128 bitów skrótu SHA256 zakodowane jako ciąg base64

Uwaga: Obiekt wpisów zawiera obecnie tylko skrót, ale w celu zapewnienia kompatybilności ze zmianami w przyszłości wybrano obiekt, a nie tablicę json.

9.5.1.2.2.2. Kody odpowiedzi

Kod	Opis
200	Wszystko ok.
410	Partia wykorzystana (ang. gone). Partia może zostać usunięta w krajowym systemie zaplecza.

9.5.1.2.2.3. Nagłówki odpowiedzi

Nagłówek	Opis
ETag	Numer identyfikacyjny partii (ang. Batch ID).

9.5.1.2.3. Punkt końcowy przesłania partii

Przesyłanie odbywa się w tym samym punkcie końcowym za pośrednictwem czasownika POST (ang. POST Verb):

/revocation-list

Verb: POST

Accepts: application/cms

Request: CMS with Content

ContentType: application/cms

Content:

{

‘country’: ‘XY’,

‘expires’: ‘2022-11-01T00:00:00Z’,

‘kid’:’23S+33f=’,

'hashType':'SIGNATURE',

'entries':[{

'hash':'e2e2e2e2e2e2e2e2'

}, ..]

}

Partię należy podpisać za pomocą certyfikatu NB_{UP}. Brama sieciowa sprawdza, czy podpis został ustawiony przez NB_{UP} dla danego *państwa*. Jeżeli kontrola podpisu nie powiodła się, przesłanie nie powiedzie się.

UWAGA: Każda partia jest niezmienna (ang. immutable) i nie może być zmieniana po przesłaniu. Można ją jednak usunąć. Przechowuje się ID każdej usuniętej partii, a przesłanie nowej partii o tym samym ID zostaje odrzucone.

9.5.1.2.4. Punkt końcowy usuwania partii

Partia może zostać usunięta z tego samego punktu końcowego za pośrednictwem czasownika DELETE (ang. DELETE Verb):

/revocation-list

Verb: DELETE

Accepts: application/cms

ContentType: application/cms

Request: CMS with Content

Content:

{

'batchId': '...'

}

lub, ze względu na kompatybilność, do następującego punktu końcowego z czasownikiem POST:

/revocation-list/delete

Verb: POST

Accepts: application/cms

ContentType: application/cms

Request: CMS with Content

Content:

{

'batchId': '...'

}

9.6. **Ochrona API/RODO**

W niniejszej sekcji określono środki służące wdrożeniu w celu zapewnienia zgodności z przepisami rozporządzenia (UE) 2021/953 w odniesieniu do przetwarzania danych osobowych.

9.6.1. *Istniejące uwierzytelnianie*

Obecnie brama sieciowa wykorzystuje certyfikat NB_{TLS} do uwierzytelniania państw łączących się z bramą sieciową. Uwierzytelnienie to można wykorzystać do określenia tożsamości państwa podłączonego do bramy sieciowej. Tożsamość tę można następnie wykorzystać do wdrożenia kontroli dostępu.

9.6.2. *Kontrola dostępu*

Aby móc zgodnie z prawem przetwarzać dane osobowe, brama sieciowa musi wdrożyć mechanizm kontroli dostępu.

Brama sieciowa wdraża wykaz kontroli dostępu połączony z zabezpieczeniem opartym na rolach. W tym systemie należy zachować dwie tabele – jedną tabelę opisującą, które role mogą stosować które operacje do których zasobów, a drugą tabelę opisującą, które role są przypisane do których użytkowników.

W celu przeprowadzenia kontroli wymaganych w niniejszym dokumencie wymagane są trzy role, tj.:

RevocationListReader

RevocationUploader

RevocationDeleter

Następujące punkty końcowe sprawdzają, czy użytkownik posiada rolę RevocationListReader; jeżeli tak, wówczas dostęp zostanie przyznany, jeżeli nie, wówczas zostanie zwrócony komunikat HTTP 403 Forbidden:

GET/revocation-list/

GET/revocation-list/{batchId}

Następujące punkty końcowe muszą sprawdzić, czy użytkownik (ang. User) posiada rolę (ang. Role) RevocationUploader; jeżeli tak, wówczas dostęp zostanie przyznany, jeżeli nie, wówczas zostanie zwrócony komunikat HTTP 403 Forbidden:

POST/revocation-list

Następujące punkty końcowe muszą sprawdzić, czy użytkownik posiada rolę RevocationDeleter; jeżeli tak, wówczas dostęp zostanie przyznany, jeżeli nie, wówczas zostanie zwrócony komunikat HTTP 403 Forbidden:

DELETE/revocation-list

POST/revocation-list/delete

Brama sieciowa zapewnia również wiarygodną metodę, dzięki której administratorzy mogą zarządzać rolami powiązanymi z użytkownikami w taki sposób, aby zmniejszyć prawdopodobieństwo wystąpienia błędów ludzkich, nie obciążając jednocześnie administratorów funkcjonalnych.”

ZAŁĄCZNIK II

Sekcja 3 załącznika V do decyzji wykonawczej (UE) 2021/1073 otrzymuje brzmienie:

„3. ***Wspólne struktury i wymagania ogólne***

Nie wydaje się unijnego cyfrowego zaświadczenia COVID, jeżeli ze względu na brakujące informacje nie wszystkie pola danych można prawidłowo wypełnić zgodnie z niniejszą specyfikacją. **Powyższego nie należy interpretować jako wpływającego na obowiązek państw członkowskich w zakresie wydawania unijnych cyfrowych zaświadczeń COVID.**

Informacje we wszystkich polach można podawać przy użyciu pełnego zestawu znaków UNICODE 13.0 zakodowanych przy użyciu UTF-8, chyba że znaki te wyraźnie ograniczają się do zestawów wartości lub węższych zestawów znaków.

Wspólna struktura jest następująca:

„JSON":{

„ver":<informacje dotyczące wersji>,

„nam":{

<informacje dotyczące imienia i nazwiska osoby>

},

„dob":<data urodzenia>,

„v" lub „t" lub „r":[

{<dawka szczepionki lub informacja o badaniu lub powrocie do zdrowia, jeden wpis>}

]

}

Szczegółowe informacje na temat poszczególnych kategorii i pól przedstawiono w kolejnych sekcjach.

W przypadku gdy przepisy wskazują, że pole powinno zostać pominięte, oznacza to, że jego zawartość musi być pusta i że ani nazwa, ani wartość pola nie są dozwolone w treści.

3.1. ***Wersja***

Należy podać informacje na temat wersji. Zapisywanie wersji następuje zgodnie z wersjonowaniem semantycznym (ang. Semantic Versioning) (semver: https://semver.org). W czasie wydawania zaświadczenia powinna to być jedna z oficjalnie opublikowanych wersji (aktualna lub jedna ze starszych oficjalnie opublikowanych wersji). Więcej informacji na ten temat znajduje się w sekcji dotyczącej lokalizacji schematu JSON (ang. JSON Schema).

ID pola	Nazwa pola	Instrukcje
ver	Wersja schematu	Odpowiada identyfikatorowi wersji schematu wykorzystywanej na potrzeby sporządzania unijnych cyfrowych zaświadczeń COVID-19. Przykład: „ver":„1.3.0"

3.2. ***Imię i nazwisko oraz data urodzenia osoby***

Imię i nazwisko osoby to oficjalne pełne imię i nazwisko osoby, odpowiadające imieniu i nazwisku podanym w dokumentach podróży. Identyfikatorem struktury jest *nam*. Należy podać imię i nazwisko dokładnie 1 (jednej) osoby.

ID pola	Nazwa pola	Instrukcje
nam/fn	Nazwisko(-a)	Nazwisko(-a) posiadacza. Jeżeli posiadacz nie ma nazwiska, a ma imię, pole należy pominąć. We wszystkich pozostałych przypadkach należy podać dokładnie 1 (jedno) pole, które nie jest puste, zawierające wszystkie nazwiska. W przypadku kilku nazwisk należy je oddzielić spacją. Nazwiska wieloczłonowe zawierające łączniki lub podobne znaki muszą jednak pozostać niezmienione.

		Przykłady: „fn":„Musterfrau-Gößinger" „fn":„Musterfrau-Gößinger Müller"
nam/fnt	Znormalizowane nazwisko (-a)	Nazwisko(-a) posiadacza transliterowane przy zastosowaniu tej samej konwencji jak konwencja stosowana w dokumentach podróży posiadacza odczytywanych maszynowo (np. zasady określone w ICAO Doc 9303 część 3). Jeżeli posiadacz nie ma nazwiska, a ma imię, pole należy pominąć. We wszystkich pozostałych przypadkach należy podać dokładnie 1 (jedno) pole, które nie jest puste, zawierające wyłącznie znaki A-Z i <. Maksymalna długość: 80 znaków (zgodnie ze specyfikacją ICAO 9303). Przykłady: „fnt":„MUSTERFRAU<GOESSINGER" „fnt":„MUSTERFRAU<GOESSINGER<MUELLER"
nam/gn	Imię(-ona)	Imię(-ona) posiadacza. Jeżeli posiadacz nie ma imienia, a ma nazwisko, pole należy pominąć. We wszystkich pozostałych przypadkach należy podać dokładnie 1 (jedno) pole, które nie jest puste, zawierające wszystkie imiona. W przypadku kilku imion należy je oddzielić spacją. Przykład: „gn":„Isolde Erika"
nam/gnt	Znormalizowane imię(-ona)	Imię(-ona) posiadacza transliterowane przy zastosowaniu tej samej konwencji jak konwencja stosowana w dokumentach podróży posiadacza odczytywanych maszynowo (np. zasady określone w ICAO Doc 9303 część 3). Jeżeli posiadacz nie ma imienia, a ma nazwisko, pole należy pominąć. We wszystkich pozostałych przypadkach należy podać dokładnie 1 (jedno) pole, które nie jest puste, zawierające wyłącznie znaki A-Z i <. Maksymalna długość: 80 znaków. Przykład: „gnt":„ISOLDE<ERIKA"
dob	Data urodzenia	Data urodzenia posiadacza cyfrowego zaświadczenia COVID (DCC) Pełna lub częściowa data bez godziny w przedziale od 1900-01-01 do 2099-12-31. Jeżeli znana jest pełna lub częściowa data urodzenia, należy podać dokładnie 1 (jedno) pole, które nie jest puste. „Jeżeli data urodzenia nie jest znana nawet częściowo, pole ustawia się jako pusty ciąg ". Powyższe powinno odpowiadać informacjom podanym w dokumentach podróży. Jeżeli dostępne są informacje o dacie urodzenia, stosuje się jeden z poniższych formatów ISO 8601. Inne formaty nie są obsługiwane. YYYY-MM-DD YYYY-MM YYYY (Aplikacja weryfikatora może wykazywać brakujące części daty urodzenia przy zastosowaniu konwencji XX takiej jak konwencja stosowana w dokumentach podróży odczytywanych maszynowo, np. 1990-XX–XX.) Przykłady: „dob":„1979-04-14" „dob":„901-08" „dob":„1939" „dob":„"

3.3. ***Kategorie informacji specyficznych dla danego typu zaświadczenia***

W schemacie JSON obsługiwane są trzy kategorie pozycji obejmujące informacje specyficzne dla danego typu zaświadczenia. Każde unijne cyfrowe zaświadczenie COVID-19 zawiera dokładnie 1 (jedną) kategorię. Puste kategorie nie są dozwolone.

Identyfikator kategorii	**Nazwa kategorii**	**Pozycje**
v	Kategoria »szczepienie«	Jeżeli występuje, musi zawierać dokładnie 1 (jedną) pozycję opisującą dokładnie 1 (jedną) dawkę szczepionki (jedną dawkę).
t	Kategoria »test«	Jeżeli występuje, musi zawierać dokładnie 1 (jedną) pozycję opisującą dokładnie 1 (jeden) wynik testu.
r	Kategoria »powrót do zdrowia«	Jeżeli występuje, musi zawierać dokładnie 1 (jedną) pozycję zawierającą 1 (jedno) oświadczenie dotyczące powrotu do zdrowia.”

ZAŁĄCZNIK III

„ZAŁĄCZNIK VI

OBOWIĄZKI PAŃSTW CZŁONKOWSKICH JAKO WSPÓŁADMINISTRATORÓW W ODNIESIENIU DO BRAMY SIECIOWEJ UNIJNEGO CYFROWEGO ZAŚWIADCZENIA COVID NA POTRZEBY WYMIANY LIST UNIEWAŻNIONYCH CERTYFIKATÓW DCC

SEKCJA 1

Podsekcja 1

Podział obowiązków

1) Współadministratorzy przetwarzają dane osobowe za pośrednictwem bramy sieciowej ram zaufania zgodnie ze specyfikacjami technicznymi zawartymi w załączniku I.

2) Organy wydające w państwach członkowskich pozostają jedynym administratorem w zakresie gromadzenia, wykorzystywania, ujawniania i wszelkiego innego przetwarzania informacji o unieważnieniu poza bramą sieciową, w tym w odniesieniu do procedury prowadzącej do unieważnienia zaświadczenia.

3) Każdy administrator odpowiada za przetwarzanie danych osobowych za pośrednictwem bramy sieciowej zgodnie z art. 5, 24 i 26 ogólnego rozporządzenia o ochronie danych.

4) Każdy administrator ustanawia punkt kontaktowy posiadający funkcyjną skrzynkę pocztową, która będzie służyć do komunikacji między samymi współadministratorami oraz między współadministratorami a podmiotem przetwarzającym.

5) Powołana przez komitet grupa robocza, o której mowa w art. 14 rozporządzenia (UE) 2021/953, jest upoważniona do podejmowania decyzji w sprawie wszelkich kwestii wynikających z wymiany list unieważnionych certyfikatów oraz ze współadministrowania powiązanego przetwarzania danych osobowych, a także do ułatwiania skoordynowanych instrukcji dla Komisji jako podmiotu przetwarzającego. Proces podejmowania decyzji przez współadministratorów podlega tej grupie roboczej i regulaminowi, który ma zostać przez nią przyjęty. Podstawową zasadą jest, że brak uczestnictwa przez któregokolwiek ze współadministratorów w posiedzeniu tej grupy roboczej, które zostało ogłoszone co najmniej siedem (7) dni przed jego zwołaniem na piśmie, oznacza milczącą zgodę na wyniki tego posiedzenia grupy roboczej. Każdy ze współadministratorów może zwołać posiedzenie tej grupy roboczej.

6) Instrukcje dla podmiotu przetwarzającego są wysyłane przez punkt kontaktowy któregokolwiek z współadministratorów w porozumieniu z pozostałymi współadministratorami, zgodnie z procesem decyzyjnym grupy roboczej, o którym mowa w pkt 5 powyżej. Współadministrator, który wydaje instrukcje, powinien przekazać je podmiotowi przetwarzającemu na piśmie i poinformować o tym wszystkich pozostałych współadministratorów. Jeżeli omawiana kwestia jest na tyle pilna, że nie pozwala na posiedzenie grupy roboczej, o którym mowa w pkt 5 powyżej, można mimo to wydać instrukcje, ale grupa robocza może je unieważnić. Instrukcje te powinny być wydawane na piśmie, a wszyscy pozostali współadministratorzy powinni być o tym informowani w momencie wydawania instrukcji.

7) Grupa robocza ustanowiona zgodnie z pkt 5 powyżej nie wyklucza indywidualnych kompetencji współadministratorów do informowania swojego właściwego organu nadzorczego zgodnie z art. 33 i 24 ogólnego rozporządzenia o ochronie danych. Takie powiadomienie nie wymaga zgody żadnego z pozostałych współadministratorów.

8) W zakresie ram zaufania dostęp do wymienianych danych osobowych mogą mieć wyłącznie osoby upoważnione przez wyznaczone organy krajowe lub organy urzędowe.

9) Każdy organ wydający prowadzi rejestr czynności przetwarzania, za które jest odpowiedzialny. W rejestrze tym można wskazać współadministrację.

Podsekcja 2

Obowiązki i role w zakresie rozpatrywania wniosków osób, których dane dotyczą, oraz w zakresie informowania takich osób

1) Każdy administrator danych pełniący rolę organu wydającego przekazuje osobom fizycznym, których zaświadczenia unieważnił („osoby, których dane dotyczą"), informacje o odnośnym unieważnieniu i przetwarzaniu ich danych osobowych w bramie sieciowej unijnych cyfrowych zaświadczeń COVID w celu wsparcia wymiany list unieważnionych certyfikatów zgodnie z art. 14 ogólnego rozporządzenia o ochronie danych, chyba że okaże się to niemożliwe lub wymaga niewspółmiernie dużego wysiłku.

2) Każdy administrator pełni rolę punktu kontaktowego dla osób fizycznych, których zaświadczenie unieważnił i rozpatruje wnioski składane przez osoby, których dane dotyczą, lub ich przedstawicieli w ramach wykonywania ich praw zgodnie z ogólnym rozporządzeniem o ochronie danych. Jeżeli współadministrator otrzyma od osoby, której dane dotyczą, wniosek dotyczący zaświadczenia wydanego przez innego współadministratora, informuje osobę, której dane dotyczą, o tożsamości i danych kontaktowych tego współadministratora. Jeżeli zostaną o to poproszeni przez innego współadministratora, współadministratorzy pomagają sobie nawzajem w rozpatrywaniu wniosków osób, których dane dotyczą, i udzielają sobie nawzajem odpowiedzi bez zbędnej zwłoki, przy czym nie później niż w terminie jednego miesiąca od otrzymania prośby o udzielenie pomocy. Jeżeli wniosek dotyczy danych przedłożonych przez państwo trzecie, administrator, który otrzymuje wniosek, rozpatruje go i informuje osobę, której dane dotyczą, o tożsamości i danych kontaktowych organu wydającego w państwie trzecim.

3) Każdy administrator udostępnia osobom, których dane dotyczą, treść niniejszego załącznika, w tym ustalenia określone w pkt 1 i 2.

SEKCJA 2

Zarządzanie cyberincydentami, w tym naruszeniami ochrony danych osobowych

1) Współadministratorzy pomagają sobie nawzajem w identyfikacji cyberincydentów i reagowaniu na nie, w tym w przypadku naruszeń ochrony danych osobowych, w związku z przetwarzaniem za pośrednictwem bramy sieciowej unijnego cyfrowego zaświadczenia COVID.

2) Współadministratorzy w szczególności powiadamiają się nawzajem o kwestiach takich, jak:

   a) wszelkie potencjalne lub faktyczne ryzyko dla dostępności, poufności lub integralności danych osobowych przetwarzanych za pośrednictwem bramy sieciowej ram zaufania;

   b) każde naruszenie ochrony danych osobowych, prawdopodobne konsekwencje naruszenia ochrony danych osobowych oraz ocena ryzyka naruszenia praw i wolności osób fizycznych, a także wszelkie środki wdrożone w celu przeciwdziałania naruszaniu ochrony danych osobowych i łagodzenia ryzyka naruszenia praw i wolności osób fizycznych;

   c) każde naruszenie technicznych lub organizacyjnych zabezpieczeń dotyczących operacji przetwarzania za pośrednictwem bramy sieciowej ram zaufania.

3) Współadministratorzy powiadamiają o wszelkich naruszeniach ochrony danych osobowych odnoszących się do operacji przetwarzania za pośrednictwem bramy sieciowej ram zaufania Komisję, właściwe organy nadzorcze i, jeśli jest to wymagane, osoby, których dane dotyczą, zgodnie z art. 33 i 34 ogólnego rozporządzenia o ochronie danych lub po otrzymaniu powiadomienia ze strony Komisji.

4) Każdy organ wydający wdraża odpowiednie środki techniczne i organizacyjne, mające na celu:

   a) zapewnienie i ochronę dostępności, integralności i poufności wspólnie przetwarzanych danych osobowych;

   b) ochronę danych osobowych będących w jego posiadaniu przed wszelkiego rodzaju przetwarzaniem, utratą, wykorzystaniem, ujawnieniem lub nabyciem, które jest nieuprawnione lub niezgodne z prawem, lub przed nieuprawnionym lub niezgodnym z prawem dostępem do tych danych;

   c) zapewnienie, aby dostęp do danych osobowych nie był ujawniany ani nie był umożliwiany nikomu innemu niż odbiorcom lub podmiotom przetwarzającym.

SEKCJA 3

Ocena skutków dla ochrony danych

1) Jeżeli administrator, w celu wypełnienia swoich obowiązków określonych w art. 35 i 36 rozporządzenia (UE) 2016/679, potrzebuje informacji od innego administratora, wysyła specjalny wniosek na adres funkcyjnej skrzynki pocztowej, o której mowa w sekcji 1 podsekcja 1 pkt 4. Administrator, który otrzymał taki wniosek, dokłada wszelkich starań, aby takie informacje przekazać."

ZAŁĄCZNIK IV

„ZAŁĄCZNIK VII

OBOWIĄZKI KOMISJI JAKO PODMIOTU PRZETWARZAJĄCEGO DANE W ODNIESIENIU DO BRAMY SIECIOWEJ UNIJNEGO CYFROWEGO ZAŚWIADCZENIA COVID NA POTRZEBY WSPIERANIA WYMIANY LIST UNIEWAŻNIONYCH CERTYFIKATÓW DCC

Komisja:

1) Tworzy i zapewnia bezpieczną i niezawodną infrastrukturę łączności w imieniu państw członkowskich, która wspiera wymianę list unieważnionych certyfikatów przedkładanych w bramie sieciowej unijnych cyfrowych zaświadczeń COVID.

2) Aby wywiązać się ze swoich obowiązków jako podmiotu przetwarzającego w ramach bramy sieciowej ram zaufania dla państw członkowskich, Komisja może angażować osoby trzecie jako podwykonawców podmiotu przetwarzającego; Komisja informuje współadministratorów o wszelkich zamierzonych zmianach dotyczących dodania lub zastąpienia innych podwykonawców podmiotu przetwarzającego, dając tym samym współadministratorom możliwość wspólnego wyrażenia sprzeciwu wobec takich zmian. Komisja zapewnia, aby do podwykonawców podmiotu przetwarzającego zastosowanie miały takie same obowiązki dotyczące ochrony danych jak te określone w niniejszej decyzji.

3) Przetwarza dane osobowe wyłącznie na udokumentowane polecenie administratorów, chyba że obowiązek taki nakłada na nią prawo Unii lub prawo państwa członkowskiego; w takim przypadku przed rozpoczęciem czynności przetwarzania Komisja informuje współadministratorów o tym obowiązku prawnym, o ile prawo to nie zabrania udzielania takiej informacji z uwagi na ważny interes publiczny;

   Przetwarzanie danych przez Komisję obejmuje:

   a) uwierzytelnianie krajowych serwerów wewnętrznych (ang. back-end servers) na podstawie krajowych certyfikatów serwerów wewnętrznych;

   b) odbiór danych, o których mowa w art. 5a ust. 3 decyzji, przesłanych przez krajowe serwery wewnętrzne poprzez zapewnienie interfejsu programowania aplikacji, który umożliwia krajowym serwerom wewnętrznym przesyłanie odpowiednich danych;

   c) przechowywanie danych w bramie sieciowej unijnego cyfrowego zaświadczenia COVID;

   d) udostępnianie danych do pobrania przez krajowe serwery wewnętrzne;

   e) usuwanie danych z datą ich wygaśnięcia lub na polecenie administratora, który je przedłożył;

   f) po zakończeniu świadczenia usługi usuwanie wszelkich pozostałych danych, chyba że prawo Unii lub prawo państwa członkowskiego nakazują przechowywanie danych osobowych.

4) Wprowadzenie wszelkich najnowocześniejszych organizacyjnych, fizycznych i logicznych środków bezpieczeństwa służących utrzymaniu bramy sieciowej unijnego cyfrowego zaświadczenia COVID. W tym celu Komisja:

   a) wyznacza podmiot odpowiedzialny za zarządzanie bezpieczeństwem na poziomie bramy sieciowej unijnego cyfrowego zaświadczenia COVID, przekazuje współadministratorom dane kontaktowe tego podmiotu oraz zapewnia jego dostępność w celu reagowania na zagrożenia dla bezpieczeństwa;

   b) przyjmuje odpowiedzialność za bezpieczeństwo bramy sieciowej unijnych cyfrowych zaświadczeń COVID, w tym za regularne przeprowadzanie testów, ocen i badań środków bezpieczeństwa;

   c) zapewnia, aby wszystkie osoby, którym przyznano dostęp do bramy sieciowej unijnego cyfrowego zaświadczenia COVID, podlegały umownemu, zawodowemu lub ustawowemu obowiązkowi zachowania poufności.

5) Wprowadza wszystkie niezbędne środki bezpieczeństwa, aby nie dopuścić do zakłócenia sprawnego funkcjonowania operacyjnego krajowych serwerów wewnętrznych. W tym celu Komisja wprowadza szczególne procedury związane z połączeniem serwerów wewnętrznych z bramą sieciową unijnego cyfrowego zaświadczenia COVID. Procedury te obejmują:

   a) procedurę oceny ryzyka, by wykryć i oszacować potencjalne zagrożenia dla systemu;

   b) procedurę audytu i przeglądu, aby:

      i. sprawdzać zgodność między wprowadzonymi środkami bezpieczeństwa a mającą zastosowanie polityką bezpieczeństwa;

      ii. przeprowadzać regularne kontrole integralności plików systemowych, parametrów bezpieczeństwa i przyznanych zezwoleń;

iii. monitorować w celu wykrywania naruszeń bezpieczeństwa i włamań;

iv. wdrażać zmiany, których celem jest ograniczenie istniejących uchybień w zakresie bezpieczeństwa;

v. określić warunki w zakresie upoważniania, w tym na wniosek administratorów, do przeprowadzania niezależnych audytów, w tym kontroli, oraz przeglądów środków bezpieczeństwa, oraz wnoszenia wkładu w przeprowadzanie tych audytów, kontroli i przeglądów, z zastrzeżeniem warunków, które są zgodne z Protokołem (nr 7) do TFUE w sprawie przywilejów i immunitetów Unii Europejskiej;

c) zmianę procedury kontroli, by udokumentować i zmierzyć wpływ zmiany przed jej wdrożeniem oraz na bieżąco informować współadministratorów o wszelkich zmianach, które mogą wpłynąć na łączność z ich infrastrukturą lub na bezpieczeństwo ich infrastruktury;

d) ustanowienie procedury konserwacji i naprawy, by określić zasady i warunki, których należy przestrzegać w przypadku konieczności przeprowadzenia konserwacji lub naprawy sprzętu;

e) ustanowienie procedury dotyczącej cyberincydentów na potrzeby określenia systemu zgłaszania i eskalacji, informowania administratorów, których to dotyczy, bezzwłocznego informowania administratorów, aby mogli poinformować krajowe organy nadzorcze ds. ochrony danych o wszelkich naruszeniach ochrony danych osobowych, a także na potrzeby określenia procesu dyscyplinarnego w przypadku naruszeń zasad bezpieczeństwa.

6) Wprowadza najnowocześniejsze fizyczne lub logiczne środki bezpieczeństwa w odniesieniu do obiektów, w których znajduje się sprzęt bramy sieciowej unijnego cyfrowego zaświadczenia COVID, oraz w odniesieniu do kontroli dostępu do danych logicznych i kontroli bezpiecznego dostępu. W tym celu Komisja:

a) egzekwuje bezpieczeństwo fizyczne, by ustanowić wyraźne granice bezpieczeństwa i umożliwić wykrywanie naruszeń;

b) kontroluje dostęp do obiektów i prowadzi rejestr odwiedzających do celów identyfikacyjnych;

c) zapewnia, aby osobom z zewnątrz, którym udzielono dostępu do obiektów, towarzyszył odpowiednio upoważniony członek personelu;

d) zapewnia, aby sprzętu nie można było dodać, wymienić ani usunąć bez uprzedniej zgody wyznaczonych odpowiedzialnych podmiotów;

e) kontroluje dostęp z oraz do krajowych serwerów wewnętrznych do bramy sieciowej ram zaufania;

f) zapewnia, aby osoby, które uzyskują dostęp do bramy sieciowej unijnego cyfrowego zaświadczenia COVID, zostały zidentyfikowane i uwierzytelnione;

g) dokonuje przeglądu uprawnień do udzielania zezwoleń na dostęp do bramy sieciowej unijnego cyfrowego zaświadczenia COVID w przypadku wykrycia naruszenia bezpieczeństwa mającego wpływ na tę infrastrukturę;

h) zachowuje integralność informacji przekazywanych za pośrednictwem bramy sieciowej unijnego cyfrowego zaświadczenia COVID;

i) wprowadza techniczne i organizacyjne środki bezpieczeństwa, by zapobiec nieuprawnionemu dostępowi do danych osobowych;

j) w razie potrzeby wdraża środki mające na celu zablokowanie nieupoważnionego dostępu do bramy sieciowej unijnego cyfrowego zaświadczenia COVID z domeny organów wydających (tj.: zablokowanie lokalizacji/adresu IP).

7) Podejmuje działania w celu ochrony swojej domeny, obejmujące zerwanie połączeń, w przypadku znacznych odstępstw od zasad i koncepcji jakości lub bezpieczeństwa;

8) Utrzymuje plan zarządzania ryzykiem związany ze swoim zakresem odpowiedzialności;

9) Monitoruje – w czasie rzeczywistym – wydajność wszystkich komponentów usług w ramach bramy sieciowej ram zaufania, tworzy regularne statystyki i prowadzi rejestry.

10) Zapewnia wsparcie w odniesieniu do wszystkich usług w ramach bramy sieciowej ram zaufania– w języku angielskim, całodobowo, przez siedem dni w tygodniu, drogą telefoniczną, mailową lub za pośrednictwem portalu internetowego – oraz odbiera połączenia od upoważnionych osób dzwoniących: koordynatorów bramy sieciowej unijnego cyfrowego zaświadczenia COVID-19 i ich odpowiednich punktów informacyjnych, specjalistów ds. projektów i wyznaczonych osób z Komisji.

11) W miarę możliwości wspiera współadministratorów za pomocą odpowiednich środków technicznych i organizacyjnych zgodnie z art. 12 rozporządzenia (UE) 2018/1725 w wywiązywaniu się z obowiązku odpowiadania na żądania osoby, której dane dotyczą, w zakresie wykonywania jej praw określonych w rozdziale III ogólnego rozporządzenia o ochronie danych.

12) Wspiera współadministratorów poprzez przekazywanie im informacji na temat bramy sieciowej unijnego cyfrowego zaświadczenia COVID w celu realizacji obowiązków przewidzianych w art. 32, 33, 34, 35 i 36 ogólnego rozporządzenia o ochronie danych.

13) Zapewnia, aby dane przetwarzane w ramach bramy sieciowej unijnego cyfrowego zaświadczenia COVID były niemożliwe do odczytania dla każdej osoby, która nie jest uprawniona do uzyskania do nich dostępu.

14) Wprowadza wszelkie odpowiednie środki, by zapobiec sytuacji, w której operatorzy bramy sieciowej unijnego cyfrowego zaświadczenia COVID mogliby uzyskać nieuprawniony dostęp do przekazywanych danych.

15) Wprowadza środki mające na celu ułatwienie interoperacyjności i łączności między wyznaczonymi administratorami bramy sieciowej unijnego cyfrowego zaświadczenia COVID.

16) Prowadzi rejestr czynności przetwarzania dokonywanych w imieniu współadministratorów zgodnie z art. 31 ust. 2 rozporządzenia (UE) 2018/1725."