Uzasadnienie

I. Wstęp

Projektowana ustawa ma na celu dostosowanie polskiego porządku prawnego do zmian, jakie zostały wprowadzone do rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014[1] – zwanego dalej „rozporządzeniem eIDAS" – rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2024/1183[2].

Celem projektowanych regulacji jest wydanie przepisów, w aktach rangi ustawowej, odnoszących się do nowych kwestii wskazanych przez znowelizowanym rozporządzeniu eIDAS, pozostających w kompetencji państw członkowskich tak, aby umożliwić prawidłową realizację tego rozporządzenia.

Kluczową nowością w rozporządzeniu eIDAS zapewnienie europejskiego portfela tożsamości cyfrowej – zwanego dalej „portfelem" – wszystkim osobom fizycznym i prawnym w Unii Europejskiej. Portfel ma umożliwić tym osobom:

- bezpieczny, zaufany i niezakłócony dostęp transgraniczny do usług publicznych i prywatnych,
- pełną kontrolę nad swoimi danymi[3].

Rozporządzenie eIDAS ustanawia najważniejsze wymogi dla portfela oraz dla dodatkowych przedsięwzięć, bez których portfel ten nie będzie mógł poprawnie funkcjonować lub być w pełni wykorzystywany. Rozporządzenie eIDAS odsyła ponadto w wielu kwestiach do obligatoryjnych lub fakultatywnych aktów wykonawczych, wydawanych przez Komisję Europejską, wskazujących właściwe normy referencyjne odnoszące się do tych wymogów, oraz, w razie potrzeby, ustanawiających dodatkowe specyfikacje i procedury.

Do najważniejszych przedsięwzięć wymaganych do zrealizowania przez państwa członkowskie, oprócz zapewnienia samego portfela, należy zaliczyć:

- udostępnienie i zapewnienie funkcjonowania rejestru stron ufających portfelowi, w którym proces rejestracji musi być efektywny kosztowo i jednocześnie proporcjonalny względem zagrożeń[4],
- zrealizowanie wymogu wskazania podmiotów wydających stronom ufającym portfelowi certyfikaty potwierdzające ich tożsamość względem portfela oraz zakres danych, jakich mogą żądać od użytkownika portfela[5],
- udostępnienie publicznych źródeł autentycznych kwalifikowanym dostawcom usług zaufania tak, aby mogli oni, na żądanie użytkownika portfela, potwierdzić atrybuty odnoszące się do tego użytkownika[6],
- zrealizowanie wymogu zgłoszenia określonych rodzajów atrybutów polegających na publicznych źródłach autentycznych do katalogu Komisji Europejskiej, ze wskazaniem adresu elektronicznego, pod którym można zweryfikować te atrybuty[7],

---

[1] 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. UE. L. z 2014 r. Nr 257, str. 73, Dz. Urz. UE L 333 z 27.12.2022, str. 80 oraz Dz. Urz. UE L 2024/1183 z 30.04.2024).

[2] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/1183 z dnia 11 kwietnia 2024 r. w sprawie zmiany rozporządzenia (UE) nr 910/2014 w odniesieniu do ustanowienia europejskich ram tożsamości cyfrowej (Dz.Urz.UE.L z 2024 r. str. 1183).

[3] Zob. art. 5a ust. 1 rozporządzenia eIDAS.

[4] Zob. art. 5b ust. 1 i 2 rozporządzenia eIDAS.

[5] Zob. przepisy wykonawcze wydane na podstawie art. 5b ust. 11 rozporządzenia eIDAS.

[6] Zob. art. 45e rozporządzenia eIDAS.

[7] Zob. przepisy wykonawcze wydane na podstawie art. 45e ust. 2 rozporządzenia eIDAS,

- zapewnienie dopasowywania tożsamości w usługach krajowych osobom korzystającym ze środków identyfikacji elektronicznej wydanych poza granicami kraju(w tym osobom mającym nadany numer PESEL i osobom, którym numeru PESEL nie nadano)[8],
- zapewnienie użytkownikom portfela możliwości nieopłatnego składania kwalifikowanego podpisu elektronicznego[9],
- przygotowanie krajowego programu certyfikacji portfela i przeprowadzenie certyfikacji portfela zgodnie z tym programem[10].

Rozporządzenie eIDAS i przepisy wykonawcze wydane na podstawie tego rozporządzenia zawierają kwestie wymagające podjęcia przez państwa członkowskie UE działań mających na celu dostosowanie krajowych usług online i systemów teleinformatycznych. Tym samym, jeżeli przepisy krajowe ograniczają zakres stosowania środków identyfikacji elektronicznej, podpisów elektronicznych, elektronicznych poświadczeń atrybutów lub innych narzędzi, jakie zostały ustanowione przepisami rozporządzenia eIDAS, to powinny one zostać odpowiednio dostosowane.

W celu zapewnienia wysokiego poziomu ochrony danych osobowych i tym samym dobrania odpowiednich środków techniczno-organizacyjnych została dokonana ocena skutków dla ochrony danych osobowych.

II. Zapewnienie wszystkim osobom fizycznym i prawnym w Polsce co najmniej jednego europejskiego portfela tożsamości cyfrowej

Państwa członkowskie zobowiązane są, zgodnie z art. 5a ust. 1 rozporządzenia eIDAS, do zapewnienia możliwości korzystania z co najmniej jednego europejskiego portfela tożsamości cyfrowej. Zgodnie z art. 5a ust. 2 tego rozporządzenia, taki portfel powinien być zapewniony w co najmniej jeden z następujących sposobów:

- bezpośrednio przez państwo członkowskie,
- na podstawie upoważnienia od państwa członkowskiego,
- niezależnie od państwa członkowskiego, lecz uznawany przez państwo członkowskie[11].

Powyższe trzy sposoby zapewnienia portfela są takie same jak sposoby wydawania środków identyfikacji elektronicznej wydawanych w ramach notyfikowanych systemów identyfikacji elektronicznej, jakie wskazano w rozporządzeniu eIDAS już w 2014 r.[12].

Mając ponadto na uwadze, że europejski portfel tożsamości cyfrowej jest w szczególności środkiem identyfikacji elektronicznej[13] i w związku z tym wymaganym jest wskazanie organu lub organów odpowiedzialnych za system identyfikacji elektronicznej, w ramach którego ten portfel (jako ten środek identyfikacji elektronicznej) jest wydawany, niezależnie od tego, w jaki sposób wydanie portfela następuje[14], przyjęto założenie, że w Polsce europejski portfel tożsamości cyfrowej zapewni minister właściwy do spraw informatyzacji, który już zapewnia funkcjonowanie systemu teleinformatycznego zapewniającego obsługę publicznego systemu identyfikacji elektronicznej.

Istotne znaczenie dla proponowanych w projekcie rozwiązań ma również to, że aplikację mObywatel, która ma podobne funkcjonalności, jakich wymaga się od europejskiego portfela tożsamości cyfrowej posiada już ponad 11 milionów użytkowników. Aplikacja mObywatel

[8] Zob. art. 11a rozporządzenia eIDAS,
[9] Zob. art. 5a ust. 5 lit. g rozporządzenia eIDAS,
[10] Zob. art. 5c rozporządzenia eIDAS,
[11]Zob. art. 5a ust. 1 i 2 rozporządzenia eIDAS,
[12] Art. 7 lit. a rozporządzenia eIDAS obowiązujący od 2014 r.
[13] Wynika to z definicji określonej w art. 3 pkt 42 rozporządzenia eIDAS
[14] Zob. art. 5d ust. 2 lit d rozporządzenia eIDAS.

zapewnia możliwość potwierdzenia tożsamości użytkownika zarówno zdalnie w usługach online, jak i podczas obecności fizycznej. Aplikacja ta umożliwia także potwierdzenie niektórych atrybutów użytkowników oraz złożenie podpisu elektronicznego. Dlatego też funkcjonujące w przestrzeni publicznej porównania aplikacji mObywatel do europejskiego portfela tożsamości cyfrowej są uzasadnione.

W przypadku aplikacji mObywatel, tożsamość i obywatelstwo polskie użytkownika aplikacji mObywatel w relacjach wzajemnej fizycznej obecności stron potwierdza „dokument mObywatel", o którym mowa w art. 2 pkt 8 ustawy z dnia 26 maja 2023 r. o aplikacji mObywatel, obsługiwany przy użyciu usługi udostępnianej w aplikacji mObywatel. W przypadku europejskiego portfela tożsamości cyfrowej, tożsamość i obywatelstwo użytkownika (nie tylko obywatela polskiego) potwierdzają dane identyfikujące osobę, o których mowa w art. 3 pkt 3 rozporządzenia eIDAS, oraz w rozporządzeniu wykonawczym Komisji (UE) 2024/2977 z dnia 28 listopada 2024 r. w sprawie ustanowienia zasad stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 w odniesieniu do danych identyfikujących osobę i elektronicznych poświadczeń atrybutów wydawanych europejskim portfelom tożsamości cyfrowej (Dz. U. UE. L. z 2024 r. poz. 2977) – zwanym dalej „rozporządzeniem 2024/2977" – wydanym na podstawie art. 5a ust. 23 rozporządzenia eIDAS.

W przypadku aplikacji mObywatel udostępnianą formą „poświadczeń elektronicznych", które potwierdzają dane użytkowników (lub rzeczy, które do tych użytkowników należą) są dokumenty mobilne w rozumieniu art. 2 ust. 8 ustawy z dnia 26 maja 2023 r. o aplikacji mObywatel. Dokumenty te uzyskiwane są przez użytkowników dzięki możliwemu połączeniu aplikacji mObywatel z systemem teleinformatycznym podmiotu, w którym są przetwarzane dane użytkownika aplikacji mObywatel, w zakresie niezbędnym do zapewnienia pobrania takich danych bezpośrednio na urządzenie mobilne tego użytkownika. Pobranie takich danych odbywa się za pośrednictwem systemu mObywatel, ale dane te nie pozostają w tym systemie teleinformatycznym. W praktyce zatem nie ma instytucjonalnego pośrednika, który wydaje tego rodzaju dokumenty, są one bowiem zapewniane od razu w aplikacji mObywatel dzięki możliwości wspomnianego wyżej pobrania danych przez użytkownika bezpośrednio ze zintegrowanego systemu teleinformatycznego, przy użyciu którego prowadzony jest rejestr w którym przetwarzane są te dane.

W przypadku europejskiego portfela tożsamości cyfrowej dokumenty elektroniczne potwierdzające dane użytkowników lub rzeczy, które do tych użytkowników należą, będą co do zasady elektronicznymi poświadczeniami atrybutów, które mogą wydawać:

- kwalifikowani dostawcy usług zaufania,
- podmioty odpowiedzialne za źródła autentyczne zawierające dane o użytkowniku, który chce uzyskać elektroniczne poświadczenie atrybutów,
- podmiot publiczny uprawniony do wydawania elektronicznych poświadczeń atrybutów w imieniu podmiotu odpowiedzialnego za źródło autentyczne.

Szczególnego podkreślenia wymaga, że różnice techniczno-organizacyjne pomiędzy aplikacją mObywatel i europejskim portfelem tożsamości cyfrowej – jaki ma być opracowany i udostępniany, zgodnie z wymogami ostatecznie określonymi w przepisach wykonawczych do rozporządzenia eIDAS i normach Europejskiego Instytutu Norm Telekomunikacyjnych[15] znacząco wpływają na możliwości uznania dzisiejszych rozwiązań aplikacji mObywatel jako odpowiadające na te wymagania.

W początkowej fazie europejski portfel tożsamości cyfrowej zostanie udostępniony jako rozwiązanie zintegrowane z obecną aplikacją mObywatel, a w późniejszym etapie jako jej

[15] European Telecommunications Standards Institute, ETSI, zob. https://www.etsi.org/

aktualizacja. Zapewnienie użytkownikom aplikacji mObywatel komfortowego przejścia do europejskiego portfela tożsamości cyfrowej będzie wyzwaniem nie tylko techniczno-organizacyjnym, ale również informacyjnym. Będzie to proces rozciągnięty w czasie.

Jednocześnie projektowana ustawa zawiera przepis, zgodnie z którym funkcjonalności aplikacji mObywatel i europejskiego portfela tożsamości cyfrowej mogą być zapewniane przez ministra właściwego do spraw informatyzacji w ramach jednego rozwiązania techniczno-organizacyjnego. Należy podkreślić, że to użytkownicy aplikacji mObywatel sami zdecydują o tym, czy chcą korzystać z europejskiego portfela tożsamości cyfrowej, ponieważ nie będzie to narzędzie obowiązkowe. Z drugiej strony istnieje szereg podmiotów, którym zgodnie z rozporządzeniem 910/2014 należy zapewnić dostęp do europejskiego portfela tożsamości cyfrowej, a które nie mają prawa do korzystania z aplikacji mObywatel. Odnotowania wymaga, że mimo udostępnienia europejskiego portfela tożsamości cyfrowej dostęp do usług publicznych i prywatnych nadal będzie musiał być możliwy z wykorzystaniem innych, istniejących środków identyfikacji i uwierzytelniania[16]

Zaproponowano, żeby krajowe przepisy wskazujące sposób zapewnienia tego portfela znalazły się w ustawie o aplikacji mObywatel. Pozostałe kwestie, jakie należy uregulować na poziomie krajowym, w związku z nowelizacją rozporządzenia eIDAS, zostaną umocowane w ustawie z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej (Dz. U. z 2024 r. poz. 1725 oraz z 2026 r. poz. 252), która jest aktem prawnym już obecnie implementującym wymagania, jakie wobec państw członkowskich formułowane były dotychczas na gruncie rozporządzenia eIDAS. W ustawie tej zostaną uregulowane następujące kwestie:

- dopasowywanie tożsamości w usługach transgranicznych, o czym mowa w art. 11a rozporządzenia eIDAS,
- funkcjonowanie rejestru stron ufających portfelowi, o którym mowa w art. 5b rozporządzenia eIDAS,
- wskazanie podmiotów wydających stronom ufającym portfelowi certyfikaty potwierdzające ich tożsamość względem europejskich portfeli tożsamości cyfrowej[17],
- udostępnianie publicznych źródeł autentycznych kwalifikowanym dostawcom usług zaufania tak, aby mogli oni, na żądanie użytkownika portfela, potwierdzić atrybuty odnoszące się do tego użytkownika, o czym mowa w art. 45e rozporządzenia eIDAS,
- zasady zgłaszania określonych rodzajów atrybutów polegających na publicznych źródłach autentycznych do katalogu prowadzonego przez Komisję Europejską, ze wskazaniem adresu elektronicznego, pod którym będzie można zweryfikować te atrybuty[18],
- zasady zgłaszania schematów poświadczania atrybutów do katalogu prowadzonego przez Komisję Europejską[19] oraz do krajowego katalogu schematów poświadczania atrybutów,
- wydawanie przez ministra właściwego do spraw informatyzacji elektronicznych poświadczeń atrybutów w imieniu podmiotów odpowiedzialnych za źródła autentyczne na podstawie schematów poświadczania atrybutów zgłoszonych do katalogu

[16] Wymóg wynikający z art. 56 ust. 15 rozporządzenia eIDAS.
[17] Wymogi wskazane w rozporządzeniu wykonawczym Komisji (UE) 2025/848 z dnia 6 maja 2025 r. ustanawiające zasady stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 w odniesieniu do rejestracji stron ufających portfela (Dz. U. UE. L. z 2025 r. poz. 848), zwanym dalej „rozporządzeniem 2025/848".
[18] Wymogi wskazane w rozporządzeniu wykonawczym Komisji (UE) 2025/1569 z dnia 29 lipca 2025 r. w sprawie ustanowienia zasad stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 w odniesieniu do kwalifikowanych elektronicznych poświadczeń atrybutów oraz elektronicznych poświadczeń atrybutów wydanych przez podmiot sektora publicznego odpowiedzialny za źródło autentyczne lub w jego imieniu (Dz. U. UE. L. z 2025 r. poz. 1569), dalej zwanym „rozporządzeniem 2025/1569".
[19] Wymogi wynikające z rozporządzenia 2025/1569.

prowadzonego przez Komisję Europejską i elektronicznych poświadczeń atrybutów ważnych tylko w kraju,
- nakładanie kar pieniężnych na dostawców usług zaufania naruszających przepisy rozporządzenia 910/2014.

III. Zmiany w ustawie z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej

Poszerzono zakres przedmiotowy ustawy do zakresu umożliwiającego realizację nowych wymagań, jakie nakłada na państwa członkowskie znowelizowane rozporządzenie eIDAS.

Ustalono zasady dokonywania wpisów do rejestru stron ufających i na zaufaną listę niekwalifikowanych usług zaufania mających znaczenie dla funkcjonowania europejskiego portfela tożsamości cyfrowej. W szczególności dotyczy to usług wydawania certyfikatów dostępu strony ufającej portfelowi oraz certyfikatów rejestracji strony ufającej portfelowi, usług wydawania niekwalifikowanych podpisów lub pieczęci elektronicznych tworzonych na odległość oraz usług wydawania do europejskiego portfela tożsamości cyfrowej niekwalifikowanych elektronicznych poświadczeń atrybutów, o których mowa w art. 3 pkt 44 i 46 rozporządzenia eIDAS.

Umożliwiono kwalifikowanym dostawcom usług zaufania wydającym kwalifikowane certyfikaty podpisu elektronicznego i kwalifikowane certyfikaty pieczęci elektronicznej, wydawanie certyfikatów dostępu strony ufającej portfelowi oraz certyfikatów rejestracji strony ufającej portfelowi. Będzie to możliwe na wniosek o wpis do rejestru usług zaufania, składany do ministra właściwego do spraw informatyzacji w trybie przewidzianym obecnie dla innych usług zaufania. Mając na uwadze dotychczasowe doświadczenia kwalifikowanych dostawców usług zaufania, zdobyte przy świadczeniu usług związanych z wydawaniem oraz obsługą pieczęci elektronicznych i podpisów elektronicznych, przyjęto, że podmioty te w profesjonalny i bezpieczny sposób obsłużą również wydawanie certyfikatów niezbędnych do funkcjonowania europejskich portfeli tożsamości cyfrowej. Certyfikaty dostępu i certyfikaty rejestracji wydaje się bowiem stronom ufającym portfelowi w celu umożliwienia tym podmiotom potwierdzania swojej tożsamości wobec użytkowników portfela oraz zakresu danych, jakiego te strony ufające będą oczekiwać od użytkownika portfela, w ramach każdej ze świadczonych usług[20].

Certyfikaty dostępu strony ufającej portfela oraz certyfikaty rejestracji strony ufającej portfela włączono do obecnie funkcjonującej krajowej infrastruktury zaufania, tak aby były one opatrywane zaawansowaną pieczęcią elektroniczną dostawcy usług zaufania, podobnie jak wymaga się tego w przypadku certyfikatów związanych ze świadczeniem kwalifikowanych usług zaufania. Taki wymóg jest uzasadniony znaczeniem tych certyfikatów dla możliwości polegania na europejskich portfelach tożsamości cyfrowej.

Poszerzono zakres danych, jakie mogą być przetwarzane na węźle krajowym identyfikacji elektronicznej, o dane, jakie potencjalnie mogą być wysłane w ramach danych identyfikujących osobę, o których mowa w rozporządzeniu 2024/2977. Określono również zakres danych odnoszących się do osób prawnych, jakie potencjalnie mogą być wysłane w ramach danych identyfikujących osobę prawną, o których mowa w rozporządzeniu 2024/2977.

Projektowane przepisy mają na celu zapewnienie użytkownikom środków identyfikacji elektronicznej – wydanych w systemach identyfikacji elektronicznej przyłączonych do węzła krajowego identyfikacji elektronicznej – możliwość zapoznania się z zapisami w dziennikach systemów (logach) odzwierciedlających historię użycia wydanych im środków identyfikacji elektronicznej wykorzystywanych za pośrednictwem węzła krajowego identyfikacji

[20] Zdefiniowanie tych certyfikatów i wymóg wskazania kto je wydaje wynika z rozporządzenia 2025/848.

elektronicznej. Celem tej usługi jest zapewnienie rozwiązania, które pozwoli użytkownikom środków identyfikacji elektronicznej, wydanych w systemach identyfikacji elektronicznej, przyłączonych do węzła krajowego identyfikacji elektronicznej, na uzyskanie podobnej informacji, jaką – zgodnie z art. 5a ust. 4 lit. d rozporządzenia eIDAS – zapewniają europejskie portfele tożsamości cyfrowej w ramach dostępu do rejestru transakcji przeprowadzonych z wykorzystaniem tych portfeli. Dostęp taki będzie ograniczony wyłącznie do danych pozwalających na zidentyfikowanie usługi online, użytego środka identyfikacji elektronicznej, z którego skorzystał użytkownik, oraz daty i czasu użycia środka identyfikacji elektronicznej. Takie dane pozwolą użytkownikom podjąć działania zmniejszające dotychczasowe i przyszłe skutki kradzieży tożsamości oraz nieuprawnionego korzystania ze środków identyfikacji elektronicznej przez przestępców. Zważywszy na to, że w Polsce możliwe jest potwierdzenie tożsamości w usługach publicznych bezpośrednio za pomocą środków identyfikacji elektronicznej wydawanych przez kilkaset podmiotów[21], usługa tego rodzaju ma istotne znaczenie. Usługa będzie dostępna wyłącznie dla osób, których dotyczą udostępniane dane, a uzyskanie dostępu do takiej usługi będzie wymagało uwierzytelnienia przy użyciu środka identyfikacji elektronicznej, wydanego w systemie identyfikacji elektronicznej przyłączonym do węzła krajowego identyfikacji elektronicznej, który spełnia wymagania określone dla wysokiego poziomu bezpieczeństwa..

W ramach projektu uwzględniono umożliwienie opracowania i udostępnienia przez ministra właściwego do spraw informatyzacji dedykowanych usług online wpierających składanie:

- wniosków o zgłoszenie, przez tego ministra, atrybutów lub schematów elektronicznych poświadczeń atrybutów do odpowiednich katalogów prowadzonych przez Komisję Europejską, oraz
- wniosków o przyłączenie systemu teleinformatycznego, w którym udostępniane są usługi online, do węzła krajowego identyfikacji elektronicznej i usług wspierających składanie i weryfikację podpisów elektronicznych.

W ramach zmian w ustawie z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej określono w jaki sposób zapewniane będzie dopasowywanie tożsamości użytkowników, którzy będą posługiwać się środkami identyfikacji elektronicznej, wydanymi w innych państwach członkowskich UE, w celu ich uwierzytelniania w usługach online w Polsce. Aby ułatwić dopasowywanie tożsamości, przewidziano uruchomienie systemu scentralizowanego, o którym mowa w rozporządzeniu wykonawczym Komisji (UE) 2025/846 z dnia 6 maja 2025 r. ustanawiającym zasady stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 w odniesieniu do transgranicznego dopasowywania tożsamości osób fizycznych (Dz. U. UE. L. z 2025 r. poz. 846), zwanym dalej „rozporządzeniem 2025/846”. System ten zapewni weryfikację danych z danymi w rejestrze PESEL, celem ustalenia, czy osoba fizyczna posiada już nadany numer PESEL (tylko w przypadkach, gdy strona ufająca wymaga podania numeru PESEL). Jeżeli numer PESEL zostanie ustalony na podstawie dopasowania danych , system dopasowania tożsamości przekaże, przez węzeł krajowy identyfikacji elektronicznej, zestaw danych oczekiwany przez stroną ufającą. W przypadku niedopasowania tożsamości w systemie scentralizowanym, dane zostaną przekazane do strony ufającej przez węzeł krajowy identyfikacji elektronicznej w formacie przewidzianym dla tego węzła i dalej w celu dopasowania strona ufająca będzie musiała podjąć próby dopasowania tożsamości w sposób zgodny z przepisami rozporządzenia 2025/846, w tym w szczególności założyć konto dla nowego użytkownika. Proponowane rozwiązanie znacząco ułatwi uwierzytelnianie użytkowników posługujących się zagranicznymi

[21] Zob. Rejestr dostawców środka identyfikacji elektronicznej przyłączonych do węzła krajowego identyfikacji elektronicznej: https://mc.bip.gov.pl/wezel-krajowy-zintegrowani-dostawcy-srodka-identyfikacji/rejestr-dostawcow-srodka-identyfikacji-elektronicznej-przylaczonych-do-wezla-krajowego.html

środkami identyfikacji elektronicznej, w przypadku gdy kiedykolwiek mieli nadany nr PESEL. Rozwiązanie to jest dedykowane obywatelom RP, którzy wyemigrowali z kraju, oraz byłym rezydentom, którzy otrzymali numer PESEL. W odniesieniu do osób, które nigdy nie miały nadanego numeru PESEL, zakłada się, że publiczne usługi online będą stopniowo dostosowywane w sposób pozwalający na zakładanie kont dla nowych użytkowników, którzy nie mają nadanego numeru PESEL. Powyższe założenie wynika bezpośrednio z przepisów rozporządzenia eIDAS i aktów wykonawczych do tego rozporządzenia , stąd też nie wymaga regulacji na gruncie krajowym.

Nowe przepisy wprowadzane do ustawy z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej implementują ponadto wymagania, o których mowa w art. 5b rozporządzenia eIDAS i przepisach wykonawczych do tego rozporządzenia. Obowiązkiem wynikającym z art. 5b rozporządzenia eIDAS jest utworzenie rejestru podmiotów, które będą chciały świadczyć swoje usługi uwzgledniające wykorzystanie europejskiego portfela tożsamości cyfrowej (rejestru stron ufających). Szczegółowo kwestie zostały uregulowane w rozporządzeniu 2025/848. Zgodnie z art. 5b ust. 2 rozporządzenia eIDAS, proces rejestracji musi być efektywny kosztowo i jednocześnie proporcjonalny względem zagrożeń, a w szczególności ma być, o ile to możliwe, zautomatyzowany[22]. Dlatego też zakłada się, że strony ufające będą mogły samodzielnie wpisywać się do rejestru i modyfikować swoje wpisy. Będą mogły w tym celu złożyć wniosek z wykorzystaniem formularza elektronicznego udostępnionego przez ministra właściwego do spraw informatyzacji. Aby wyjść naprzeciw wskazanym powyżej wytycznym, dotyczącym procesu rejestracji, wniosek będzie możliwy do złożenia po uwierzytelnieniu wnioskodawcy za pomocą środka identyfikacji osoby prawnej albo zaawansowanej pieczęci elektronicznej weryfikowanej za pomocą kwalifikowanego certyfikatu.

Przewiduje się również zapewnienie możliwości składania wyżej wspomnianego wniosku, do ministra właściwego do spraw informatyzacji, za pośrednictwem kwalifikowanego dostawcy usług zaufania świadczącego usługę wydawania certyfikatów dostępu strony ufającej portfelowi lub certyfikatów rejestracji strony ufającej portfelowi, o których mowa w rozporządzeniu 2025/848. Takie rozwiązanie umożliwi stronom ufającym załatwienie wszystkich formalności, niezbędnych do polegania na portfelu, (tj. wpisu do rejestru i uzyskania wyżej wspomnianych certyfikatów) w jednym miejscu.

Wpis do rejestru stron ufających będzie następował automatycznie, po zweryfikowaniu kompletności danych przekazanych za pomocą formularza elektronicznego, udostępnionego przez ministra właściwego do spraw informatyzacji lub w ramach wniosku, przekazanego za pośrednictwem kwalifikowanego dostawcy usług zaufania. Zakłada się bowiem, że zakres danych osobowych, jakich strona ufająca będzie żądać od użytkownika europejskiego portfela tożsamości cyfrowej, nie będzie urzędowo weryfikowany w postępowaniu administracyjnym przed dokonaniem wpisu do rejestru stron ufających, ponieważ będzie wyświetlony każdemu użytkownikowi portfela, korzystającemu z danej usługi. Oznacza to, że sami użytkownicy portfela będą mieli możliwość zweryfikowania, czy żąda się od nich nadmiarowych danych i będą mogli poinformować o takim ewentualnym przypadku organ ochrony danych osobowych za pomocą usługi udostępnionej w każdym portfelu. Taki samoregulujący się system zapewni minimalizację danych niezbędnych do świadczenia usług bez potrzeby biurokratyzowania kwestii dostępu do tych wyżej wspomnianych danych w kosztownym postępowaniu administracyjnym, które spowalniałoby proces rejestracji, a jednocześnie nie zapewniłoby w praktyce lepszej ochrony takich danych.

[22] zgodnie z art. 6 ust. 1 rozporządzenia wykonawczego Komisji (UE) 2025/848

Specjalną procedurę postępowania przewiduje się w sytuacjach, gdy wniosek zawiera wskazanie pośrednika, o którym mowa w pkt 14 i 15 załącznika I do rozporządzenia 2025/848. Mając na uwadze wytyczne określone w art. 5b ust. 2 rozporządzenia eIDAS (tj. wymaganie, że proces musi być efektywny kosztowo i proporcjonalny względem zagrożeń) oraz w art. 6 ust. 1 rozporządzenia wykonawczego Komisji (UE) 2025/848 (tj. wymaganie, że proces ma być, o ile to możliwe, zautomatyzowany), nie przewiduje się badania przez organ rejestrujący autentyczności i treści umów dotyczących pośrednictwa, o którym mowa w art. 5b ust. 10 rozporządzenia eIDAS, oraz w pkt 14 i 15 załącznika I do rozporządzenia 2025/848, jakie podmiot wnioskujący zawarł z pośrednikiem wpisanym do rejestru krajowego. W takim przypadku wpis będzie następował automatycznie, po potwierdzeniu deklarowanego pośrednictwa przez wskazanego pośrednika, który zostanie uprzednio uwierzytelniony w systemie teleinformatycznym, w ramach którego prowadzony jest rejestr. Tylko w przypadkach, gdy wskazany pośrednik, o którym mowa w pkt 14 i 15 załącznika I do rozporządzenia 2025/848, będzie wpisany do rejestru stron ufających prowadzonego w innym państwie członkowskim UE, do wniosku będzie wymagane załączenie elektronicznego odpisu umowy – poświadczonego przez notariusza oraz sporządzonego w języku polskim – który umożliwi organowi rejestrującemu dokonanie wpisu do rejestru.

W związku z tym, że strona ufająca będzie musiała uzyskać certyfikat dostępu, który będzie wydawany przez krajowe podmioty świadczące kwalifikowane usługi zaufania oraz certyfikaty rejestracji strony ufającej portfela, które będą mogły być wydane przez te podmioty , rejestr będzie musiał w szczególności zapewnić automatyczne powiadamianie wystawców takich certyfikatów o konieczności ich unieważnienia po dokonaniu zmian w rejestrze, które będą uzasadniały takie unieważnienie. Projektowane przepisy, wprowadzane do ustawy z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej, dotyczą także elektronicznych poświadczeń atrybutów, o których mowa w sekcji 9 rozporządzenia eIDAS, w tym ustanawiają sposób wykonania obowiązków, nałożonych na państwa członkowskie w ramach tego rozporządzenia oraz rozporządzenia wykonawczego Komisji (UE) 2025/1569 z dnia 29 lipca 2025 r. w sprawie ustanowienia zasad stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 w odniesieniu do kwalifikowanych elektronicznych poświadczeń atrybutów oraz elektronicznych poświadczeń atrybutów wydanych przez podmiot sektora publicznego odpowiedzialny za źródło autentyczne lub w jego imieniu (Dz. U. UE. L. z 2025 r. poz. 1569) – zwanego dalej „rozporządzeniem 2025/1569”. Z definicji zawartych w art. 3 pkt 43 i 44 rozporządzenia eIDAS wynika, że „elektroniczne poświadczenie atrybutów” oznacza poświadczenie w postaci elektronicznej, które umożliwia uwierzytelnienie cechy charakterystycznej, właściwości, prawa lub zezwolenia osoby fizycznej, lub prawnej lub przedmiotu. Na uwagę zasługuje również definicja „źródła autentycznego”, którym – zgodnie z art. 3 pkt 47 rozporządzenia eIDAS – jest „repozytorium lub system, za prowadzenie którego odpowiedzialny jest podmiot sektora publicznego lub podmiot prywatny, które zawiera i udostępnia atrybuty – tj. cechy charakterystyczne, właściwości, prawa lub zezwolenia – dotyczące osoby fizycznej lub prawnej lub przedmiotu i które uważa się za podstawowe źródło tych informacji lub uznaje za autentyczne zgodnie z prawem Unii lub prawem krajowym, w tym z praktykami administracyjnymi”. Wartym odnotowanie jest, że krajowych przepisach[23] funkcjonuje pojęcie „danych referencyjnych”, rozumianych jako „dane opisujące cechę informacyjną obiektu - tj. przedmiotu opisu w rejestrze publicznym – pierwotnie wprowadzone do rejestru publicznego w wyniku określonego zdarzenia, z domniemania opatrzone atrybutem autentyczności”. Mając na uwadze, że przepisy rozporządzenia eIDAS stosuje się bezpośrednio, przyjęto założenie, że na gruncie projektowanych przepisów projektodawca

[23] W rozporządzeniu Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. poz. 773).

będzie posługiwał się terminologią określoną w tym rozporządzeniu (czyli pojęciem „źródło autentyczne”), aby nie stwarzać wątpliwości odnoszących się do kwestii, do których przepisów europejskich odnoszą się określone przepisy krajowe.

Nie funkcjonuje również w przepisach krajowych pojęcie „elektroniczne poświadczenie atrybutów”, ponieważ jest to nowa usługa zaufania, która została wprowadzona na gruncie znowelizowanego rozporządzenia eIDAS. Na uwagę zasługuje, że wydawane w aplikacji mObywatel dokumenty mobilne, zdefiniowane w art. 2 ust. 7 ustawy z dnia 26 maja 2023 r. o aplikacji mObywatel), czyli dokumenty elektroniczne obsługiwane przy użyciu usługi udostępnianej w aplikacji mObywatel, wpisują się w ogólną definicję elektronicznego poświadczenia atrybutów, określoną w art. 3 pkt 44 rozporządzenia eIDAS. Każdy dokument mobilny może być uznany za poświadczenie w postaci elektronicznej, które umożliwia uwierzytelnienie cechy charakterystycznej, właściwości, prawa lub zezwolenia osoby fizycznej lub prawnej, lub innego przedmiotu.

I w tym przypadku, mając na uwadze, że przepisy rozporządzenia eIDAS stosuje się bezpośrednio, przyjęto założenie posługiwania się terminologią określoną w tym rozporządzeniu.

Zgodnie z rozporządzeniem eIDAS elektroniczne poświadczenia atrybutów mogą być wydawane jako:

a) kwalifikowane elektroniczne poświadczenie atrybutów - wydawane przez kwalifikowanych dostawców usług zaufania, spełniające wymagania określone w załączniku V do rozporządzenia eIDAS;
b) elektroniczne poświadczenie atrybutów wydane przez podmiot sektora publicznego odpowiedzialny za źródło autentyczne lub w jego imieniu –wydawane przez podmiot publiczny odpowiedzialny za źródło autentyczne lub przez podmiot publiczny, który jest wyznaczony przez państwo członkowskie do wydawania takich poświadczeń w imieniu podmiotu odpowiedzianego za źródło autentyczne, spełniające wymagania określone w załączniku VII do rozporządzenia eIDAS;
c) pozostałe elektroniczne poświadczenia atrybutów, które nie muszą spełniać wymagań, o których mowa wyżej w lit. a i b.

Elektroniczne poświadczenia atrybutów nie muszą być wydawane wyłącznie do europejskich portfeli tożsamości cyfrowej. Nie ma bowiem takiego ograniczenia w żadnym z przepisów, a pośrednio potwierdza to pkt 3 załącznika II do rozporządzenia 2025/1569. Jeżeli jednak takie poświadczenia będą wydawane do europejskich portfeli tożsamości cyfrowej, to zgodnie z art. 8 rozporządzenia wykonawczego Komisji (UE) 2024/2979 z dnia 28 listopada 2024 r. ustanawiającego zasady stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 w odniesieniu do integralności i podstawowych funkcji europejskich portfeli tożsamości cyfrowej (Dz. U. UE. L. z 2024 r. poz. 2979), będą musiały być wydawane w formatach danych wskazanych w załączniku II do tego rozporządzenia. Takie wymagania są uzasadnione potrzebą zapewnienia interoperacyjności europejskich portfeli tożsamości cyfrowej i elektronicznych poświadczeń atrybutów używanych za pośrednictwem tych portfeli.

W związku z powyższym, proponowane nowe przepisy, wprowadzane do ustawy z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej, wskazują, kto będzie wykonywał obowiązki, o których mowa w art. 45e ust. 1 rozporządzenia eIDAS, czyli zapewniał kwalifikowanym dostawcom usług zaufania, którzy będą dostarczali kwalifikowane elektroniczne poświadczenia atrybutów, możliwość weryfikacji drogą elektroniczną, na żądanie użytkownika, atrybutów, o których mowa w załączniku VI do rozporządzenia eIDAS. Z uwagi na to, że nie istnieje obecnie żadna krajowa platforma umożliwiająca weryfikację tak rozległego zakresu danych, zakłada się, że co do zasady możliwość weryfikacji danych drogą

elektroniczną będą realizowały podmioty publiczne, które są odpowiedzialne na poziomie krajowym za poszczególne źródła autentyczne – każdy podmiot we własnym zakresie. Nie wyznacza się pośredników, którzy mogliby, zamiast podmiotów odpowiedzialnych za źródła autentyczne, weryfikować atrybuty, tym niemniej należy mieć na uwadze, że wprost na podstawie art. 10 rozporządzenia 2025/1569 państwa członkowskie mogą odnosić się do usług wspólnych systemu technicznego – określonego w art. 14 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2018/1724 z dnia 2 października 2018 r. w sprawie utworzenia jednolitego portalu cyfrowego w celu zapewnienia dostępu do informacji, procedur oraz usług wsparcia i rozwiązywania problemów, a także zmieniające rozporządzenie (UE) nr 1024/2012 – i ponownie wykorzystywać te wspólne usługi, a także krajowe komponenty z nimi połączone.

Wspomniane wyżej podmioty publiczne celowo nie są wymieniane wprost w projektowanych przepisach, z uwagi na to, że stale postępująca informatyzacja zadań publicznych powoduje tworzenie kolejnych publicznych źródeł autentycznych, które wcześniej nie istniały. Zakłada się, że odpowiednie podmioty publiczne udostępnią kwalifikowanym dostawcom usług zaufania zarządzane przez siebie źródła autentyczne – do weryfikacji danych na podstawie przepisów eIDAS – stąd też nie ma potrzeby dodawania takiego wymogu w przepisach sektorowych. Powodowałoby to bowiem niepotrzebną inflację prawa i dodatkowo niepewność w zakresie możliwości udostępnienia źródeł autentycznych, w przypadku, gdy nie byłoby specjalnego przepisu ustawowego wymagającego udostępnienia określonego źródła. Mogłoby to w zasadniczy sposób utrudnić albo wręcz uniemożliwić wydawanie kwalifikowanych elektronicznych poświadczeń atrybutów, co byłoby niezgodne z ogólnymi celami europejskich ram tożsamości cyfrowej.

W kontekście zapewnienia ochrony danych osobowych w procesie wspomnianej wyżej weryfikacji danych, istotne są zasady tej weryfikacji danych, określone w art. 9 ust. 3 i 4 rozporządzenia 2025/1569. Z przepisów tych wynika, że kwalifikowany dostawca usług zaufania, pytający o weryfikację atrybutów, musi wstępnie znać wartość atrybutu, o który pyta działając z upoważnienia (tj. na żądanie) użytkownika, ponieważ wynik weryfikacji może określać wyłącznie, czy atrybut został potwierdzony. Przykładowo znaczy to, że nie można zapytać „jakie wykształcenie/jaki dyplom/jakie uprawnienia ma osoba X", tylko poprosić o potwierdzenie, że osoba X ma określone wykształcenie/uzyskała dyplom określonej uczelni o określonej specjalizacji/posiada określone uprawnienia. W rezultacie weryfikacji będzie można uzyskać odpowiedź tak/nie, zamiast pakietu danych odnoszących się do danej osoby.

Obecnie, w ramach aplikacji mObywatel, funkcjonują poświadczenia dotyczące sytuacji prawnej użytkownika tej aplikacji lub praw mu przysługujących, które, wydawane są jako dokumenty mobilne. Dokumenty te są postrzegane zarówno przez użytkowników tej aplikacji, jak i przez strony ufające tym poświadczeniom jako potrzebne. W związku z powyższym, w proponowanych przepisach zakłada się, że minister właściwy do spraw informatyzacji będzie mógł wydawać elektroniczne poświadczenia atrybutów, o których mowa w art. 45f rozporządzenia eIDAS, w imieniu podmiotów odpowiedzialnych za źródła autentyczne, a w szczególności będzie mógł wydawać je do zapewnianego przez siebie europejskiego portfela tożsamości cyfrowej. Należy bowiem założyć, że jeżeli europejski portfel tożsamości cyfrowej nie będzie zapewniał co najmniej takich samych możliwości potwierdzania atrybutów, jakie obecnie zapewnia aplikacja mObywatel (za pomocą dokumentów mobilnych), może być postrzegany przez użytkowników jako narzędzie mniej użyteczne i w rezultacie nie będzie wykorzystywany.

Jak zaznaczono na wstępie ze względów techniczno-organizacyjnych nie będzie możliwe wykorzystanie istniejących dokumentów mobilnych, funkcjonujących w ramach aplikacji

mObywatel, w celu uzyskania elektronicznego poświadczenia atrybutów w europejskim portfelu tożsamości cyfrowej.

Minister właściwy do spraw informatyzacji będzie mógł wydawać elektroniczne poświadczenie atrybutów, do europejskiego portfela tożsamości cyfrowej, które będą wydawane w imieniu podmiotu sektora publicznego odpowiedzialnego za źródło autentyczne, w rozumieniu art. 3 pkt 46 rozporządzenia eIDAS (spełniające wymagania art. 45f rozporządzenia eIDAS), uznawane w całej UE, zgodnie z art. 45b ust. 2 tego rozporządzenia) lub elektroniczne poświadczenia atrybutów, w rozumieniu art. 3 pkt 44 rozporządzenia eIDAS (bez konieczności spełniania wymagań art. 45f rozporządzenia eIDAS i co za tym idzie niemające skutku zgodnego z art. 45b ust. 2 tego rozporządzenia). Zakłada się bowiem, że nie wszystkie elektroniczne poświadczenia atrybutów, wydawane przez ministra właściwego do spraw informatyzacji do zapewnianego przez niego europejskiego portfela tożsamości cyfrowej, muszą mieć skutek prawny wskazany w art. 45b ust. 2 rozporządzenia eIDAS (np. karta mieszkańca określonego miasta), jak również, że nie wszystkie z nich muszą taki skutek uzyskać z dniem wejścia w życie niniejszej ustawy (np. poświadczenie, że określona osoba jest radcą prawnym).

Ponadto, celów związku z zapewnieniem funkcjonowania elektronicznych poświadczeń atrybutów, wydawanych do europejskiego portfela tożsamości cyfrowej, ważnych wyłącznie w Polsce, przyjęto, że powstanie krajowy katalog schematów poświadczania atrybutów wzorowany na katalogu schematów prowadzonym przez Komisję Europejską, o którym mowa w art. 8 ust. 3 rozporządzenia wykonawczego Komisji (UE) 2025/1569 z dnia 29 lipca 2025 r. w sprawie ustanowienia zasad stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 w odniesieniu do kwalifikowanych elektronicznych poświadczeń atrybutów oraz elektronicznych poświadczeń atrybutów wydanych przez podmiot sektora publicznego odpowiedzialny za źródło autentyczne lub w jego imieniu.

Z uwagi na to, że procedury zgłaszania atrybutów i schematów elektronicznych poświadczeń atrybutów do właściwych katalogów prowadzonych przez Komisję Europejską, o których mowa w rozporządzeniu 2025/1569, nie zostały jeszcze praktyce zweryfikowane, jak również na to, że wnioski zgłaszające atrybuty i schematy elektronicznych poświadczeń atrybutów podlegają ocenie Komisji Europejskiej po zasięgnięciu opinii Grupy Współpracy, ustanowionej na podstawie art. 46e ust. 1 rozporządzenia eIDAS, należało ustanowić skutek prawny elektronicznych poświadczeń atrybutów, potwierdzających dany stan prawny lub uprawnienia osób posługujących się nim, wydawanych przez ministra właściwego do spraw informatyzacji, do zapewnianego przez tego ministra europejskiego portfela tożsamości cyfrowej. Zaproponowane w ustawie z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej brzmienie przepisu uwzględnia, że nie wszystkie wydawane w Polsce dokumenty potwierdzające określony stan prawny lub uprawnienia są wydawane w postaci papierowej. Celem tych przepisów nie jest możliwość potwierdzenia tożsamości osoby za pomocą elektronicznego poświadczenia atrybutów, a jedynie stanu prawnego lub uprawnień.

W projektowanych przepisach proponuje się ustalenie zasad składania wniosków o włączenie atrybutów, wymienionych w załączniku VI do rozporządzenia 910/2014, do katalogu atrybutów prowadzonego przez Komisję Europejską, oraz wniosków o włączenie schematów poświadczania atrybutów do katalogu schematów poświadczania atrybutów zapewnianego przez Komisję Europejską. Wnioski o włączenie atrybutów do katalogu atrybutów prowadzonego przez Komisję Europejską będzie co do zasady składał minister właściwy do spraw informatyzacji. Celem przyjęcia powyższego rozwiązania jest zapewnienie spójnej polityki państwa w tym zakresie.

Wnioski o włączenie schematów poświadczania atrybutów do katalogu schematów poświadczania atrybutów zapewnianego przez Komisję Europejską będzie mógł składać minister właściwy do spraw informatyzacji, podmioty odpowiedzialne za źródła autentyczne, w rozumieniu art. 3 pkt 47 rozporządzenia 910/2014, kwalifikowani dostawcy usług zaufania świadczący usługi wydawania kwalifikowanych poświadczeń atrybutów oraz dostawcy usług online, wpisani do rejestru stron ufających, gdy wpis dotyczy atrybutu, dla którego zgłaszany jest schemat.

Mając na uwadze, że składane, przez ministra właściwego do spraw informatyzacji, wnioski o włączenie atrybutów i schematów poświadczania atrybutów do odpowiednich katalogów prowadzonych przez Komisję Europejską będą wymagały wkładu przygotowanego przez podmioty odpowiedzialne za źródła autentyczne ustala się sposoby przekazywania takiego wkładu. Minister właściwy do spraw informatyzacji będzie wnioskował o włączenie atrybutu lub schematu poświadczania atrybutów do odpowiedniego katalogu Komisji Europejskiej na podstawie otrzymanego wniosku podmiotu odpowiedzialnego za źródła autentyczne.

W ramach projektowanych zmian w ustawie z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej proponuje się nałożenie na ministra właściwego do spraw informatyzacji szeregu nowych zadań informacyjnych, które wynikają z przepisów rozporządzenia eIDAS, w tym ustanowienie krajowego programu certyfikacji, w odniesieniu do wymogów, o których mowa w art. 5c ust. 3 rozporządzenia eIDAS, i wyznaczenie jednostek oceniających zgodność europejskich portfeli tożsamości cyfrowej, o których mowa w art. 5c ust. 1 rozporządzenia eIDAS.

W kontekście tych przepisów należy zwrócić uwagę, że – zgodnie z art. 5c ust. 2 rozporządzenia eIDAS – certyfikację zgodności europejskich portfeli tożsamości cyfrowej, które są związane z cyberbezpieczeństwem, przeprowadza się zgodnie z europejskimi programami certyfikacji cyberbezpieczeństwa, przyjętymi na podstawie rozporządzenia Parlamentu Europejskiego i Rady (UE) 2019/881 z dnia 17 kwietnia 2019 r. w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych oraz uchylenia rozporządzenia (UE) nr 526/2013 (akt o cyberbezpieczeństwie) (Dz. U. UE. L. z 2019 r. Nr 151, str. 15 z późn. zm.) – zwanego dalej „rozporządzeniem 2019/881" – oraz programami certyfikacji cyberbezpieczeństwa, wymienionymi w aktach wykonawczych, o których mowa w art. 5c ust. 6 rozporządzenia eIDAS[24].

Z uwagi na to, że nie zostały jeszcze wydane europejskie programy certyfikacji cyberbezpieczeństwa dla europejskich portfeli tożsamości cyfrowej, przyjęte na podstawie rozporządzenia 2019/881, certyfikacja europejskiego portfela tożsamości cyfrowej wydawanego w Polsce będzie opierała się o programy certyfikacji wydane na podstawie dwóch różnych aktów prawnych. W zakresie zgodności z cyberbezpieczeństwem, na podstawie przepisów wydanych na podstawie ustawy z dnia 25 czerwca 2025 r. o krajowym systemie certyfikacji cyberbezpieczeństwa (Dz. U. z 2026 r. poz. 20 i 252), a zakresie pozostałych elementów na podstawie ustawy z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej (Dz. U. z 2024 r. poz. 1725).

W projekcie zaproponowano także przepisy mające na celu zapewnienie rozdzielności i niezależności zadań realizowanych przez ministra właściwego do spraw informatyzacji w zakresie wydawania europejskiego portfela tożsamości cyfrowej oraz certyfikacji oraz nadzoru nad dostawcami usług zaufania oraz krajowym schematem identyfikacji

[24] Obecnie to rozporządzenie wykonawcze Komisji (UE) 2024/2981 z dnia 28 listopada 2024 r. ustanawiające zasady stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 w odniesieniu do certyfikacji europejskich portfeli tożsamości cyfrowej (Dz. U. UE. L. z 2024 r. poz. 2981).

elektronicznej. Analogicznie zapewniono rozdzielność i niezależność zadań realizowanych przez ministra właściwego do spraw informatyzacji w zakresie wydawania elektronicznych poświadczeń atrybutów oraz nadzoru nad dostawcami usług zaufania oraz krajowym schematem identyfikacji elektronicznej. Zastosowano tu podobne rozwiązanie jak w art. 4 ust. 4 ustawy z dnia 25 czerwca 2025 r. o krajowym systemie certyfikacji cyberbezpieczeństwa.

Projekt zakłada również rozszerzenie działalności akredytacyjnej Polskiego Centrum Akredytacji (PCA) zobowiązując PCA do akredytacji jednostek oceniających zgodność na potrzeby przedmiotu regulowanego na gruncie niniejszej projektowanej ustawy oraz rozporządzenia eIDAS.

IV. Zmiany w ustawie z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne

Calem proponowanych zmian w ustawie z dnia 17 lutego 2005 r. o informatyzacji podmiotów realizujących zadania publiczne (Dz. U. z 2025 r. poz. 1703 oraz z 2026 r. poz. 160) jest:

- wskazanie, że zapewniany przez ministra właściwego do spraw informatyzacji europejski portfel tożsamości cyfrowej wydaje się w ramach publicznego systemu identyfikacji elektronicznej, o którym mowa w art. 20aa tej ustawy,
- zapewnienie możliwości wydawania profilu zaufanego podmiotu publicznego oraz profilu zaufanego osoby fizycznej reprezentującej podmiot publiczny.

Z uwagi na to, że europejski portfel tożsamości cyfrowej jest środkiem identyfikacji elektronicznej[25] oraz że – zgodnie z art. 5d ust. 2 lit. b rozporządzenia eIDAS – należy przekazać Komisji Europejskiej opis systemu identyfikacji elektronicznej, w ramach którego zapewniany będzie europejski portfel tożsamości cyfrowej, zasadnym jest, aby portfel był kolejnym środkiem identyfikacji elektronicznej wydawanym w ramach publicznego systemu identyfikacji elektronicznej, który został już notyfikowany w Komisji Europejskiej, na podstawie art. 9 rozporządzenia eIDAS. Dodatkowo należy dodać, że źródłem autentycznym dla danych identyfikujących osobę będzie – podobnie jak w przypadku pozostałych środków identyfikacji elektronicznej, wydawanych w ramach publicznego systemu identyfikacji elektronicznej – rejestr PESEL. Jednocześnie, organem odpowiedzialnym za notyfikowany publiczny system identyfikacji elektronicznej i jednostką, która zarządza rejestracją niepowtarzalnych danych identyfikujących osobę oraz organem nadzoru[26] będzie ten sam podmiot, który został wskazany w projektowanych przepisach jako podmiot zapewniający w Polsce europejski portfel tożsamości cyfrowej.

W związku z powyższym należy poszerzyć zakres danych, jakie minister właściwy do spraw informatyzacji może przetwarzać w ramach publicznego systemu identyfikacji elektronicznej, gdyż zakres danych identyfikujących osobę wydawanych dla europejskiego portfela tożsamości cyfrowej wydawanego w Polsce będzie szerszy niż zakres danych dotychczas przetwarzanych w ramach tego systemu.

Istotną korzyścią, jaką daje umocowanie europejskiego portfela tożsamości cyfrowej wydawanego w Polsce jako kolejnego środka identyfikacji elektronicznej wydawanego w ramach publicznego systemu identyfikacji elektronicznej, jest zapewnienie użytkownikom tego portfela możliwości korzystania z usług publicznych przyłączonych obecnie do węzła

[25] Zgodnie z art. 3 pkt 34 rozporządzania eIDAS, "europejski portfel tożsamości cyfrowej" oznacza środek identyfikacji elektronicznej, który umożliwia użytkownikowi bezpieczne przechowywanie i walidację danych identyfikujących osobę i elektronicznych poświadczeń atrybutów oraz bezpieczne zarządzanie tymi danymi i poświadczeniami na potrzeby udostępniania ich stronom ufającym oraz innym użytkownikom europejskich portfeli tożsamości cyfrowej, i który umożliwia składanie kwalifikowanych podpisów elektronicznych lub kwalifikowanych pieczęci elektronicznych;
[26] Zob. https://ec.europa.eu/digital-building-blocks/sites/spaces/EIDCOMMUNITY/pages/554369093/Poland

krajowego identyfikacji elektronicznej. Portfel ten zostanie bowiem dołączony do wyżej wspomnianego węzła jako kolejny środek identyfikacji elektronicznej, ponieważ:

- jest środkiem identyfikacji elektronicznej w rozumieniu art. 3 pkt 42 rozporządzenia eIDAS,
- w Polsce wszystkie usługi publiczne i wszystkie środki identyfikacji elektronicznej wydane w publicznym systemie identyfikacji elektronicznej, pozwalające na korzystanie z tych usług, są przyłączone do węzła krajowego identyfikacji elektronicznej na mocy art. 21m ustawy z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej, aby zapewnić użytkownikom tych usług możliwość wyboru środka identyfikacji elektronicznej, którym dysponują, a publicznym dostawcom tych usług jednorazową integrację z tym węzłem (a nie osobno z każdym dostawcą środka identyfikacji elektronicznej).

Dzięki takiemu działaniu:

- użytkownicy zapewnianego przez ministra właściwego do spraw informatyzacji europejskiego portfela tożsamości cyfrowej od razu uzyskają możliwość korzystania ze wszystkich usług online, które obecnie są przyłączone do węzła krajowego identyfikacji elektronicznej (w szczególności usług publicznych), co będzie zgodne z oczekiwaniami tych użytkowników,
- publiczni dostawcy usług online będą gotowi na uwierzytelnianie użytkowników za pomocą portfela bez potrzeby wprowadzenia kosztownych zmian w swoich systemach (wszyscy dostawcy w jednym i tym samym czasie), oraz
- zostanie wykorzystana istniejąca już infrastruktura techniczno-organizacyjna.

Formalnie stroną ufającą wpisaną do rejestru stron ufających będzie w tym przypadku minister właściwy do spraw informatyzacji udostępniający węzeł krajowy identyfikacji elektronicznej, gdyż będzie on świadczył dla użytkowników portfela usługę przekazania przez ten węzeł zestawu danych identyfikujących osobę, w formacie przewidzianym dla tego węzła, a nie w formacie przewidzianym dla europejskiego portfela tożsamości cyfrowej. Zakłada się, że wymagany od portfela zestaw danych będzie zawsze taki sam jak obecnie we wszystkich usługach publicznych (tj.: imię, nazwisko, data urodzenia i numer PESEL) i zostanie on wpisany do rejestru stron ufających, o którym mowa w art. 5b rozporządzenia eIDAS. Gdy w ramach rozwoju usług publicznych okaże się potrzebne są inne zestawy danych lub gdy usługi te będą wykorzystywać elektroniczne poświadczenia atrybutów, to usługi te będą mogły być sukcesywnie dostosowywane do takich zmian, w szczególności aby umożliwić bezpośrednią integrację z portfelem. Taka bezpośrednia integracja z portfelem będzie już wymagała od podmiotu publicznego wpisania się do rejestru stron ufających, uzyskania certyfikatu dostępu strony ufającej portfela oraz certyfikatu rejestracji strony ufającej portfela, jak również dostosowania systemu teleinformatycznego do formatów danych przewidzianych dla komunikacji z portfelem (innych niż format danych przekazywany z węzła krajowego identyfikacji elektronicznej). Dzięki przyłączeniu do węzła krajowego identyfikacji elektronicznej wydawanego w kraju portfela, wspomniane wyżej dostosowanie nie będzie konieczne od razu i w związku z tym nie będzie powodować jednorazowego spiętrzenia się kosztów, jak również tworzenia się tzw. „wąskich gardeł" przy wdrażaniu nowych rozwiązań od strony organizacyjno-technicznej po oddaniu portfela od użytku[27]. Zakłada się, że zmiany będą następowały stopniowo w miarę potrzeb wynikających z rozwoju systemów

[27] Gdyby konieczne było przyłączenie do portfela wszystkich podmiotów publicznych w jednym czasie, spowodowałoby to konieczność dostosowania systemów publicznych do komunikacji z portfelem w jednym czasie i w efekcie masowe zamawianie usług integracyjnych, co dodatkowo zwiększyłoby koszty po stronie jednostek sektora finansów publicznych.

teleinformatycznych i tworzenia usług wykorzystujących inne niż identyfikacja elektroniczna funkcjonalności portfela.

Jeżeli chodzi o zapewnienie możliwości wydawania profilu zaufanego podmiotu publicznego oraz profilu zaufanego osoby fizycznej reprezentującej podmiot publiczny, to pierwsze z tych narzędzi będzie środkiem identyfikacji elektronicznej osoby prawnej, w rozumieniu rozporządzenia eIDAS, a drugie środkiem identyfikacji elektronicznej osoby fizycznej reprezentującej osobę prawną. Celem wydawania takich środków jest zapewnienie narzędzi, które następnie umożliwią osobom prawnym, jakimi są podmioty publiczne, i ich pracownikom, na zidentyfikowanie się w systemach teleinformatycznych jako takie właśnie osoby, bez potrzeby dodatkowego informowania strony ufającej o tym, że ma ona do czynienia z podmiotem publicznym lub jego przedstawicielem.

Dodatkową korzyścią będzie możliwość polegania w usługach publicznych na środkach identyfikacji elektronicznej pracowników podmiotów publicznych niezawierających numeru PESEL, w przypadkach gdy taki numer nie jest wymagany. W szczególności numer PESEL nie byłby przesyłany do dostawcy usługi online. Zakłada się, że do jednoznacznej identyfikacji pracownika załatwiającego sprawę wystarczy imię i nazwisko, data urodzenia oraz nazwa i numer reprezentowanego podmiotu publicznego, pod jakim podmiot ten jest zarejestrowany w Katalogu Podmiotów Publicznych. Mając na uwadze, że jest możliwe, że podmiot publiczny może być reprezentowany przez dwóch pracowników o takim samym imieniu i nazwisku, zakłada się, że data urodzenia jest w takim przypadku wystarczającym, naturalnym wyróżnikiem, który zapewni jednoznaczną identyfikację osoby fizycznej.

W celu zapewnienia równowagi pomiędzy bezpieczeństwem podmiotu publicznego i bezpieczeństwem pracownika tego podmiotu, mając przy tym na uwadze wymogi dotyczące powiązania między środkami identyfikacji elektronicznej osób fizycznych i osób prawnych, wskazane w części 2.1.4 załącznika do rozporządzenia wykonawczego Komisji (UE) 2015/1502 z dnia 8 września 2015 r. w sprawie ustanowienia minimalnych specyfikacji technicznych i procedur dotyczących poziomów zaufania w zakresie środków identyfikacji elektronicznej na podstawie art. 8 ust. 3 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym (Dz. U. UE. L. z 2015 r. Nr 235, str. 7 z późn. zm.) – zwanego dalej „rozporządzeniem 2015/1502" -wskazano, że profil zaufany podmiotu publicznego oraz profil zaufany osoby fizycznej reprezentującej podmiot publiczny są powiązane z profilami zaufanymi osoby fizycznej osób upoważnionych do używania wyżej wspomnianych profili zaufanych. Dzięki takiemu powiązaniu podmiot publiczny będzie miał pewność, że będzie go reprezentował wyłącznie upoważniony pracownik i będzie mógł w każdej chwili odwołać takie upoważnienie, a upoważniany pracownik będzie miał pewność, że podmiot publiczny, który go upoważnił, nie będzie w stanie użyć wydanego dla niego profilu zaufanego bez jego wiedzy.

W przypadku profilu zaufanego podmiotu publicznego, który umożliwia następnie potwierdzanie przez podmiot publiczny profili zaufanych osób fizycznych reprezentujących ten podmiot, wymagane jest używanie mechanizmów uwierzytelniania polegających na profilu osobistym lub kwalifikowanym certyfikacie podpisu elektronicznego. To dodatkowe wymaganie zabezpiecza podmioty publiczne przed skutkami potencjalnej kradzieży profilu zaufanego administratora wskazanego do zarządzania profilem zaufanym podmiotu publicznego. Nawet jeżeli miałoby miejsce takie zdarzenie, wymagany mechanizm uwierzytelniania spowodowałby, że profil zaufany podmiotu pozostałby bezpieczny.

Projekt przewiduje wprowadzenie przepisów dotyczących Katalogu Podmiotów Publicznych (KPP), które mają na celu zapewnienie funkcjonowania rejestru publicznego, w którym znajdą

się wszystkie aktualne i kompletne dane dotyczące pomiotów publicznych. KPP zapewni efektywną wymianę danych i współpracę między KPP a systemami teleinformatycznymi administracji publicznej, eliminując wyspowe budowanie baz danych o podmiotach publicznych wdrażane na potrzeby konkretnych systemów, ograniczy zjawisko zbędnej redundancji danych oraz zapewni wysoki poziom dostępności i otwartości danych z KPP na potrzeby ponownego wykorzystania danych przez administrację, obywateli i przedsiębiorców.

KPP będzie rejestrem publicznym, prowadzonym przez ministra właściwego do spraw informatyzacji udostępnianym podmiotom publicznym przy użyciu systemu teleinformatycznego.

KPP będzie istotnym źródłem danych dla bazy adresów elektronicznych (BAE), która posłuży do weryfikacji wniosków o nadanie adresu do doręczeń elektronicznych dla podmiotów publicznych. Z tego względu przepisy przewidują, że KPP będzie udostępniał dane za pośrednictwem interfejsu programistycznego aplikacji oraz, że będzie w jednym miejscu gromadził dane podmiotów.

Projektowane przepisy określają również zakres danych przetwarzanych w KPP, w tym określają źródła, z których dane te będą pobierane automatycznie, co ma na celu zoptymalizować proces pozyskiwania danych z zaufanych źródeł tj. rejestrów publicznych (oraz z innych oficjalnych źródeł jak strona podmiotowa podmiotu publicznego w BIP). Dane, które nie będą pozyskiwane automatycznie, będą obowiązane dostarczyć podmioty publiczne – dotyczy to danych, w których posiadaniu są podmioty i jednocześnie brak jest źródeł pozwalających na ich automatyczne pozyskanie np. dane o godzinach otwarcia/urzędowania podmiotu.

Z projektowanych przepisów wynika, że to minister właściwy do spraw informatyzacji będzie administratorem danych przetwarzanych w KPP. Minister Cyfryzacji będzie podejmował wszelkie adekwatne w tym zakresie działania i podejmował adekwatne do zagrożeń środki w celu prewencji i reagowania na zagrożenia.

Projektowane przepisy wprowadzają katalog enumeratywnie wymienionych danych podmiotów, które przetwarzane będą w KPP, w tym w szczególności dane:

1) osób fizycznych (imię, nazwisko, numer PESEL, numer telefonu, adres poczty elektronicznej, oraz adres do doręczeń elektronicznych, jeżeli został ustanowiony, wykorzystywane do realizacji obowiązków służbowych), które:

a) są uprawnione do zarządzania podmiotem,

b) administrują kontem podmiotu w KPP.

2) imię i nazwisko administratora skrzynki doręczeń podmiotu, jego adres poczty elektronicznej oraz numer PESEL, a jeżeli nie został nadany – niepowtarzalny identyfikator nadany przez państwo członkowskie Unii Europejskiej dla celów transgranicznej identyfikacji, o którym mowa w rozporządzeniu wykonawczym Komisji 2015/1501.

Jednocześnie minister właściwy do spraw informatyzacji będzie usuwał z KPP dane osobowe niezwłocznie po ich aktualizacji, wycofaniu albo wycofaniu podmiotu z Katalogu Podmiotów Publicznych, co stanowi realizację zasady ograniczenia przechowywania danych wynikającej z rozporządzenia 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. UE. L. z 2016 r. Nr 119, str. 1, z późn. zm.) i służy ochronie prywatności osób, których te dane dotyczą.

Ponadto, w zakresie danych przetwarzanych w KPP projekt ustawy przewiduje regulację polegającą na tym, że niektóre dane podmiotów publicznych, będą automatycznie przekazywane do KPP z:

1) krajowego rejestru urzędowego podmiotów gospodarki narodowej (rejestr REGON), o którym mowa w art. 42 ustawy dnia 29 czerwca 1995 r. o statystyce publicznej (Dz. U. z 2024 r. poz. 1779 oraz z 2025 r. poz. 1792);

2) krajowego rejestru urzędowego podziału terytorialnego kraju, o którym mowa w art. 47 ustawy z dnia 29 czerwca 1995 r. o statystyce publicznej;

3) bazy adresów elektronicznych (BAE);

4) ePUAP.

Z Krajowego Rejestru Sądowego dane będą udostępniane Ministrowi Cyfryzacji na potrzeby prowadzenia KPP.

Ponadto, również minister właściwy do spraw informatyzacji będzie mógł w pewnych przypadkach wprowadzać, wycofywać lub aktualizować niektóre dane o podmiotach publicznych na podstawie danych udostępnionych w Biuletynie Informacji Publicznej podmiotu publicznego lub w portalu danych, lub w innym systemie teleinformatycznym podmiotu publicznego, w trybie ustawy z dnia 11 sierpnia 2021 r. o otwartych danych i ponownym wykorzystywaniu informacji sektora publicznego (Dz. U. z 2023 r. poz. 1524), a także prostować oczywiste błędy i omyłki pisarskie.

Minister właściwy do spraw informatyzacji na wniosek podmiotu publicznego złożony w systemie teleinformatycznym, przy użyciu którego prowadzony będzie KPP, z wykorzystaniem usługi online udostępnionej przez tego ministra będzie zakładał konta dla podmiotów publicznych w KPP.

Jeżeli podmiot publiczny nie złoży wniosku to minister właściwy do spraw informatyzacji będzie mógł założyć z urzędu temu podmiotowi automatycznie konto podmiotu publicznego w KPP, na podstawie danych z rejestrów, o których mowa w brzmieniu dodawanych w art. 20w i art. 20x, albo innych powszechnie dostępnych danych i informacji. Minister właściwy do spraw informatyzacji będzie powiadamiał niezwłocznie podmiot publiczny o utworzeniu temu podmiotowi konta w KPP. Powiadomienie będzie odbywało się na adres do doręczeń elektronicznych (ADE) tego podmiotu, a w przypadku braku możliwości wysłania powiadomienia na ADE wysłane zostanie przy wykorzystaniu publicznej usługi hybrydowej (PUH).

Minister właściwy do spraw informatyzacji będzie wycofywał z KPP z urzędu podmiot publiczny w przypadku zniesienia albo likwidacji tego podmiotu.

Wycofanie, będzie stanowić czynność materialno-techniczną i wywoła skutki prawne od dnia jej dokonania. Minister właściwy do spraw informatyzacji niezwłocznie powiadomi podmiot o jego wycofaniu z KPP. Powiadomienie zostanie przekazane na ADE tego podmiotu albo przy wykorzystaniu usługi PUH – o ile będzie to możliwe.

Podmioty publiczne będą administratorami konta podmiotu w KPP w zakresie jego zarządzania i obsługi.

W zakresie uwierzytelnienia w KPP wskazano, że będzie ono następowało w sposób określony w art. 20a ust. 1 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2025 r. poz. 1703 oraz z 2026 r. poz. 160).

Podmiotom publicznym, których dane przetwarzane będą w KPP, nadawany będzie automatycznie numer identyfikacyjny w KPP.

Dodano podstawę do tworzenia przez ministra właściwego do spraw informatyzacji konta administratora podmiotu publicznego, które będzie służyło do zarządzania danymi przez podmiot wpisany do KPP.

Zgodnie z projektowanymi przepisami dane do KPP wprowadzają podmioty publiczne w terminie 5 dni roboczych od dnia odebrania korespondencji informującej o utworzeniu konta podmiotu publicznego w KPP. Jednocześnie podmioty te będą zobowiązane do aktualizacji tych danych w terminie 5 dni roboczych od dnia zmiany tych informacji.

Dane przetwarzane w KPP będą udostępniane podmiotom publicznym także za pośrednictwem interfejsu programistycznego aplikacji. W drodze decyzji administracyjnej minister właściwy do spraw informatyzacji wycofa dostęp do danych w KPP w przypadku wystąpienia ryzyka naruszenia bezpieczeństwa przez podmiot realizujący zadania publiczne.

W projektowanych przepisach wskazana została również podstawa prawna do wydania przez ministra właściwego do spraw informatyzacji rozporządzenia określającego:

1) szczegółowy zakres danych, o których mowa w dodawanym art. 20u ust. 3 pkt 1 lit. w i x,
2) szczegółowy tryb i sposób utworzenia konta podmiotu publicznego w KPP,
3) sposób zarządzania kontem administratora podmiotu publicznego w KPP

– biorąc pod uwagę konieczność zapewnienia przetwarzania aktualnych danych o podmiotach publicznych, ujednolicenie sposobu utworzenia konta podmiotu publicznego i konta administratora podmiotu publicznego w KPP, a także prawidłowość i sprawność zarządzania kontem administratora podmiotu publicznego w KPP.

Zmiana w art. 2 projektu dotyczy zmian w ustawie z dnia 29 czerwca 1995 r. o statystyce publicznej, gdzie w art. 42 dodaje się ust. 15, z którego wynika, że informacja o adresie do doręczeń elektronicznych jest przekazywana automatycznie za pośrednictwem bazy adresów elektronicznych, o której mowa w art. 25 ustawy z dnia 18 listopada 2020 r. o doręczeniach elektronicznych.

Zmiana w art. 3 projektu dotyczy zmian w ustawie z dnia 20 sierpnia 1997 r. o Krajowym Rejestrze Sądowym (Dz. U. z 2025 r. poz. 869, 1556 i 1792), gdzie w art. 20 w ust. 1c pkt 3 doprecyzowuje się przepisy dotyczące gromadzenia lub aktualizacji danych w KPP, o którym mowa w art. 20u ust. 3 ustawy z dnia 18 listopada 2020 r. o doręczeniach elektronicznych.

Z wyżej wspomnianymi zmianami w zakresie KPP związany jest również art. 10 projektu, który stanowi, że minister właściwy do spraw może utworzyć z urzędu konto podmiotu publicznego, w KPP, w terminie 12 miesięcy od dnia wejścia w życie niniejszej projektowanej ustawy, na podstawie danych z rejestrów, o których mowa w dodawanym art. 20w, albo innych danych udostępnionych w Biuletynie Informacji Publicznej na stronie podmiotowej podmiotu publicznego lub w portalu danych, lub w innym systemie teleinformatycznym podmiotu publicznego w trybie ustawy z dnia 11 sierpnia 2021 r. o otwartych danych i ponownym wykorzystywaniu informacji sektora publicznego (Dz. U. z 2023 r. poz. 1524). Minister właściwy do spraw informatyzacji będzie zamieszczał na stronie internetowej informacje o utworzeniu konta podmiotu publicznego w KPP. Podmioty publiczne, którym zostało utworzone konto podmiotu publicznego w KPP, będą składały, w terminie 30 dni od dnia zamieszczenia informacji, o której mowa w art. 10 ust. 2 projektu, wniosek, o którym mowa w brzmieniu dodawanego art. 20z ust. 1. Do wniosku będą miały zastosowanie odpowiednio przepisy dodawanego art. 20y ust. 5 i 6 oraz art. 20z ust. 2, 3 i 4.

V. Zmiany w ustawie z dnia 26 maja 2023 r. o aplikacji mObywatel

Zakres przedmiotowy regulacji ustawy ulegnie poszerzeniu o kwestie dotyczące europejskiego portfela tożsamości cyfrowej, który będzie zapewniany w Polsce.

Zmieniana ustawa będzie upoważniała ministra właściwego do spraw informatyzacji do wydawania europejskiego portfela tożsamości cyfrowej, a w tym także do zapewniania następujących, niezbędnych elementów tego portfela:

- oprogramowanie przeznaczone dla urządzeń mobilnych umożliwiające korzystanie z tego portfela,
- bezpieczną aplikację kryptograficzną portfela, o której mowa w art. 2 pkt 1 rozporządzenia 2024/2979,
- bezpieczne urządzenie kryptograficzne portfela, o którym mowa w art. 2 pkt 12 rozporządzenia 2024/2979,
- wydanie danych identyfikujących osobę.

Na gruncie zmienianej ustawy ustalony zostanie krajowy zestaw danych identyfikujących osobę fizyczną, jaki będzie znajdował się w europejskim portfelu tożsamości cyfrowej zapewnianym przez ministra właściwego do spraw informatyzacji. Zestaw ten będzie zawierał dane obowiązkowe, wynikające z przepisów rozporządzenia 2024/2977. Pozostałe dane, jakie mają znaleźć się w krajowym zestawie danych identyfikujących osobę użytkownika portfela, są wymienione w rozporządzeniu 2024/2977 jako elementy opcjonalne.

Zważywszy jednak, że:

- kompletny zestaw danych wymagany na poziomie krajowym musi zapewnić jednoznaczną identyfikacją osoby fizycznej i co za tym idzie musi być uzupełniony o elementy opcjonalne, które łącznie z danymi wymaganymi zapewnią taką identyfikację,
- rozporządzenie 2024/2977 dopuszcza możliwość włączenia do zestawu danych identyfikujących osobę elementu zwanego „personal_administrative_number” (rozumianego jako „Wartość przypisana osobie fizycznej, która jest niepowtarzalna wśród wszystkich osobistych numerów administracyjnych wydanych przez dostawcę danych identyfikujących osobę. W przypadku gdy państwa członkowskie zdecydują się na włączenie tego atrybutu, mają obowiązek opisać w swoich systemach identyfikacji elektronicznej, w ramach których wydawane są dane identyfikujące osobę, politykę, którą stosują do wartości tego atrybutu, w tym, w stosownych przypadkach, szczególne warunki przetwarzania tej wartości”),
- w Polsce numerem jednoznacznie identyfikującym osobę fizyczną jest numer PESEL

włączenie do krajowego zestawu danych identyfikujących osobę numeru PESEL jest w pełni uzasadnione.

Dzięki wykorzystaniu numeru PESEL nie będzie potrzeby dodatkowego łącznego przetwarzania z danymi obowiązkowymi w tych usługach innych danych, takich jak np.: nazwisko rodowe, adres zamieszkania, adres email, czy nr telefonu komórkowego. Często podnoszony w odniesieniu do usług online argument, że nie każda taka usługa online oraz nie każdy system teleinformatyczny wymaga identyfikacji osoby fizycznej przy użyciu numeru PESEL, a w wielu przypadkach cele przetwarzania mogą być realizowane z wykorzystaniem innych identyfikatorów lub mechanizmów uwierzytelniania, nie jest w tym przypadku wystarczający. Należy bowiem wskazać, że europejski portfel tożsamości cyfrowej bez możliwości przekazania przez użytkownika numeru PESEL w procesie uwierzytelniania stałby się narzędziem bezużytecznym dla większości użytkowników. Wobec znaczących nakładów finansowych, jakich wymaga zapewnienie obywatelom takiego portfela, opisana wyżej sytuacja nie tylko byłaby rażącą niegospodarnością, ale byłaby także niezgodna z ogólnymi celami rozporządzenia eIDAS (ułatwienie bezpiecznej elektronicznej identyfikacji

i uwierzytelniania). Niemożliwe byłoby również uzyskiwanie elektronicznych poświadczeń atrybutów w oparciu o źródła autentyczne, w których cechę charakterystyczną, właściwość, prawo lub zezwolenie osoby fizycznej powiązano z numerem PESEL.

Warto przy tym dodatkowo podkreślić, że poleganie w celu jednoznacznej identyfikacji osoby fizycznej na zmiennych elementach, takich jak adres zamieszkania, adres email, czy nr telefonu komórkowego, może spowodować uniemożliwienie ciągłego korzystanie przez taką osobę z usług online po zmianie tych danych, a w szczególności uniemożliwienie dostępu do konta w systemie teleinformatycznym, w którym takie usługi są udostępniane. W krótkim czasie pojawiłaby się potrzeba przyporządkowywania odpowiednio nowego adresu zamieszkania, adresu email lub numeru telefonu komórkowego do poprzedniego, przyjętego identyfikatora (wynikowo tworzenia historii zmian adresów i numerów), jak również przebudowy usług online w celu obsługi takich danych. Ponadto, każda zmiana adresu zamieszkania, adresu email lub numeru telefonu komórkowego wymagałaby ponownego wydania zestawu danych identyfikujących osobę i co za tym idzie ponownego potwierdzenia tożsamości, co byłoby nie tylko uciążliwe dla użytkowników nieposiadających dowodu osobistego z warstwą elektroniczną, ale również kosztowne dla państwa.

Bardzo dobrze ilustrują przyszłe problemy, jakie niosłoby ze sobą poleganie na wyżej wspomnianych, zmiennych elementach, kłopoty, jakie obecnie mają użytkownicy profilu zaufanego, którzy zmienili numer telefonu komórkowego, ale zapomnieli wpisać nowy numer do swojego profilu zaufanego, w czasie, w którym jeszcze dysponowali poprzednim numerem. Innym dobrze ilustrującym przykładem konsekwencji polegania na zmiennych danych są problemy z dostępem do usług online, jakie mają osoby fizyczne po zmianie numeru PESEL. W związku z tym, że nie ma żadnego unikatowego elementu, na którym można by polegać celem dopasowania nowej tożsamości do danych i dokumentacji tej osoby zgromadzonych wcześniej, w praktyce zmusza to do indywidualnego działania takiej osoby celem uzyskania dostępu do każdego takiego zbioru danych. Podsumowując, rezygnacja z numeru PESEL, jako unikalnego identyfikatora osoby fizycznej, i poleganie w tym zakresie na elementach zmiennych, takich jak opisane powyżej, wiązałoby się nie tylko z istotnymi problemami użytkowników w dostępie do ich danych zgromadzonych w rejestrach publicznych i systemach teleinformatycznych podmiotów publicznych, ale prowadziłoby również do konieczności kosztownej przebudowy większości usług publicznych, poprzedzonej zmianami przepisów prawa regulujących funkcjonowanie tych usług.

Ponadto, należy podkreślić, że w przypadku, gdy w usłudze online nie jest niezbędny numer PESEL, mechanizmy portfela będą pozwalały na to, aby numer PESEL nie był przekazywany. Europejskie portfele tożsamości cyfrowej mają umożliwiać selektywne udostępnianie danych, czyli działać inaczej niż inne środki identyfikacji elektronicznej wydawane w ramach publicznego systemu identyfikacji elektronicznej (tj. profilu zaufanego, profilu osobistego i profilu mObywatel), dla których zestaw danych identyfikujących osobę fizyczną jest ustalony i stały.

Podobnie będzie w przypadku nazwiska rodowego i płci jako elementów znajdujących się w krajowym zestawie danych identyfikujących osobę. Przekazywanie tych danych przez użytkownika portfela stronie ufającej będzie możliwe, tylko wtedy, gdy strona ta zarejestruje się w rejestrze stron ufających europejskiemu portfelowi tożsamości cyfrowej i wskaże odrębnie każdą usługę, w której zamierza takie dane wykorzystywać. Użytkownik portfela będzie za każdym razem informowany komu i jakie dane przekazuje i będzie mógł zablokować wysłanie takich danych oraz w wygodny sposób powiadomić organ ochrony danych o każdym nieuzasadnionym żądaniu danych, co będzie prowadziło do samoregulującego się systemu (tj. dane nadmiarowe nie będą żądane przez strony ufające z uwagi na możliwość interwencji powiadomionego, przez użytkownika portfela, organu ochrony danych).

W związku z takimi cechami portfela i otaczających go systemów teleinformatycznych i rejestrów warto zaznaczyć, że zasada minimalizacji danych, o której mowa w rozporządzeniu 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 (ogólnym rozporządzeniem o ochronie danych) (Dz. U. UE. L. z 2016 r. Nr 119, str. 1 z późn. zm.) – zwanym dalej „RODO" – w przypadku danych znajdujących się w zestawie danych identyfikujących osobę, powinna być rozumiana inaczej niż w przypadku usług online, w jakich wykorzystuje się ten portfel.

Dodanie do zestawu danych identyfikujących osobę elementu danych, jakim jest płeć, jest uzasadniona, z uwagi na fakt dodania numeru PESEL, który już zawiera oznaczenie płci. Skoro i tak oznaczenie płci będzie przetwarzane w ramach danych identyfikujących osobę, zasadnym jest, aby użytkownicy europejskiego portfela tożsamości cyfrowej, zapewnianego przez ministra właściwego do spraw informatyzacji, mogli ten element udostępniać odrębnie, wykorzystując opcję, jaką musi zapewniać każdy portfel, czyli możliwość selektywnego udostępniania danych. Dzięki temu użytkownicy portfela będą mogli udostępnić informację o płci, nie udostępniając jednocześnie numeru PESEL, a nawet żadnych innych danych, jeżeli nie będzie takiej potrzeby.

Dodanie do zestawu danych identyfikujących osobę nazwiska rodowego jest wyjściem naprzeciw możliwości tworzenia usług, w których ten element danych może być wykorzystywany do precyzyjnego ustalenia tożsamości osoby, w przypadku, gdy strona ufająca nie przetwarza numeru PESEL (na przykład w usługach transgranicznych lub w usługach krajowych, w których nazwisko rodowe jest potrzebne na podstawie przepisów odrębnych). Mając na uwadze wskazaną wyżej możliwość selektywnego ujawniania danych, istnienie w zestawie danych identyfikujących osobę nazwiska rodowego i płci może przyczynić się do minimalizacji danych używanych w usługach online, ponieważ pozwoli użytkownikowi portfela na przekazanie stronie ufającej wyłącznie takiej informacji, bez potrzeby wysyłania innych danych.

Fotografia twarzy użytkownika portfela, jako element krajowego zestawu danych identyfikujących osobę, jest niezbędny z uwagi na potrzebę zwiększenia bezpieczeństwa procesu identyfikacji podczas obecności fizycznej. Chodzi o to, aby użytkownik europejskiego portfela tożsamości cyfrowej, zapewnianego przez ministra właściwego do spraw informatyzacji, podobnie jak obecnie użytkownik dokumentu mObywatel, mógł potwierdzić swoją tożsamość, okazując, oprócz zestawu danych określających jego tożsamość, także fotografię. Zakłada się, że potwierdzenie danych podczas obecności fizycznej wymaga okazania również fotografii tak, aby strona weryfikująca tożsamość miała pewność, że dokumentem tym posługuje się ta osoba fizyczna, której dane zawiera okazywany dokument. Dzięki temu wyeliminowane zostanie niebezpieczeństwo posługiwania się europejskim portfelem tożsamości cyfrowej, zapewnianym przez ministra właściwego do spraw informatyzacji, podczas obecności fizycznej, przez osoby trzecie działające bez zgody lub wiedzy użytkownika tego portfela.

Projekt ustawy określa też zestaw danych identyfikujących osobę prawną. Wymóg zapewnienia europejskiego portfela tożsamości cyfrowej dla osoby prawnej i co za tym idzie także określenia zestawu danych identyfikujących taką osobę wynika z art. 5a ust. 1 rozporządzenia eIDAS. W projekcie zaproponowano minimalny zestaw danych, jaki jest wymagany przez rozporządzenie 2024/2977. Takie minimum danych wynika z tego, że obecnie nie są wydawane w Polsce środki identyfikacji elektronicznej osoby prawnej i co z tym idzie nie ma usług online przygotowanych do wykorzystania takich środków.

W projekcie wskazano również zestaw metadanych odnoszących się do wydawanego zestawu danych identyfikujących osobę, o którym mowa w tabeli 5 załącznika do rozporządzenia 2024/2977. Ograniczono się przy tym do trzech elementów obowiązkowych, wynikających z przepisów europejskich oraz jednego elementu opcjonalnego. Elementami obowiązkowymi będą zatem:

1) data i godzina wygaśnięcia ważności danych identyfikujących osobę,
2) nazwa organu, który wydał dane identyfikujące osobę (w przypadku zapewnianego przez ministra właściwego do spraw informatyzacji europejskiego portfela tożsamości cyfrowej będzie nim ten minister),
3) dwuznakowy kod ISO 3166-1 dla Rzeczypospolitej Polskiej.
4) numer danych identyfikujących osobę nadany przez dostawcę danych identyfikujących osobę.

W praktyce numer danych identyfikujących osobę będzie mógł mieć podobne znaczenie jak numer dokumentu mObywatel wydawany automatycznie po ustaleniu tożsamości użytkownika aplikacji mObywatel. Dane identyfikujące osobę wydane do europejskiego portfela tożsamości cyfrowej, zapewnianego przez ministra właściwego do spraw informatyzacji, będą bowiem zapewniały, zgodnie z art. 5a ust. 4 lit. a rozporządzenia eIDAS, możliwość potwierdzenia tożsamości użytkownika, w całej Unii Europejskiej, w celu uzyskania dostępu do usług publicznych i prywatnych, przy jednoczesnym zapewnieniu możliwości selektywnego ujawniania danych.

W projektowanych przepisach wskazano ponadto dwa okresy przechowywania danych osobowych użytkowników europejskiego portfela tożsamości cyfrowej zapewnianego przez ministra właściwego do spraw informatyzacji. Dane związane z rejestracją użytkownika portfela i wydaniem mu danych identyfikujących osobę, i unieważnieniem europejskiego portfela tożsamości cyfrowej, będą przechowywane przez 20 lat od dnia jego unieważnienia. Wspomniany wyżej okres przechowywania tych danych będzie taki sam, jak w przypadku danych, przechowywanych przez kwalifikowanych dostawców usług zaufania, związanych ze świadczeniem usług zaufania, dokumentów i danych związanych z wydawaniem przedłużaniem i unieważnianiem profilu zaufanego, jak również danych, które są przetwarzane w systemie identyfikacji elektronicznej, w którym jest wydawany profil mObywatel. Celem przetwarzania tych danych jest w każdym takim przypadku zapewnienie bezpieczeństwa obrotu prawnego, na wypadek gdyby zaszła potrzeba udowodnienia, że w określonym czasie funkcjonował konkretny środek identyfikacji elektronicznej, który był wydany określonej osobie lub funkcjonowała usługa zaufania, która świadczona byłą na rzecz określonej osoby, i były one ważne. W przeciwnym przypadku potwierdzenie lub zaprzeczenie autentyczności dokumentacji elektronicznej, sporządzanej z wykorzystaniem narzędzi, których istnienia w określonym czasie nie można by już potwierdzić, byłoby poważnie utrudnione lub niemożliwe. Nie przewiduje się przeglądu tych danych w celu wyselekcjonowania tych danych, które mogłyby być przechowywane krócej. Celem przechowania tych danych jest zapewnienie możliwości udowodnienia (także w sądzie), że określony portfel istniał, był aktywny i był wydany określonej osobie z zachowaniem określonych wymogów zgodnych z przepisami, stąd też niezbędne jest zachowanie całości dokumentacji. Przykładowo, w przypadku zaprzeczenia przez użytkownika jakoby w ogóle posiadał on w określonym czasie portfel, brak przechowywania jakiejkolwiek części danych lub metadanych dotyczących rejestracji użytkownika mógłby prowadzić do poważnych konsekwencji w obrocie prawnym. Podobnie, w przypadku kradzieży tożsamości, brak posiadania takich kompletnych danych mógł utrudnić lub nawet uniemożliwić ujęcie przestępców, a także uniemożliwić udowodnienie, że kradzież w ogóle miała miejsce. W konsekwencji powyższego przestępca mógłby uniknąć

odpowiedzialności za dokonane, niezgodne z prawym, czyny (takie jak na przykład zaciąganie kredytów lub innych zobowiązań wobec osób trzecich).

Ponadto, co do zasady nie powinno się dokonywać zmian w zgromadzonej dokumentacji przed upływem czasu jej przechowywania, gdyż mogłaby utracić wartość dowodową, o jaką w tym przypadku chodzi. Jednocześnie, w przypadku tego rodzaju dokumentacji całkowicie niezasadna jest pseudonimizacja danych, o której mowa w art. 89 ust. 1 RODO.

Pozostałe dane, niezbędne do świadczenia usługi europejskiego portfela tożsamości cyfrowej, umożliwiające użytkownikom takiego portfela odtworzenie rejestru transakcji przeprowadzonych z wykorzystaniem ich europejskiego portfela tożsamości cyfrowej, o którym mowa w art. 5a ust. 4 lit. d rozporządzenia eIDAS, oraz odtworzenie konfiguracji portfela na nowym urządzeniu, będą przechowywane tylko przez 2 lata. Znaczy to, że w przypadku uszkodzenia, zagubienia lub kradzieży urządzenia mobilnego użytkownika europejskiego portfela tożsamości cyfrowej, na którym zainstalował on ten portfel i zarejestrował się jako użytkownik tego portfela, będzie on mógł odtworzyć wspomniany wyżej rejestr transakcji oraz posiadane elektroniczne poświadczenia atrybutów, jednakże tylko dwa lata wstecz, a pozostałe dane zostaną bezpowrotnie utracone. Do danych umożliwiających odtworzenie rejestru transakcji będzie miał dostęp tylko zarejestrowany użytkownik portfela. Taka usługa będzie miała dla użytkownika portfela istotne znaczenie w przypadku kradzieży portfela i używania go bez jego zgody. Po odzyskaniu portfela użytkownik będzie mógł się dowiedzieć, gdzie jego portfel był używany, podczas gdy pozostawał poza jego kontrolą, oraz podjąć działania zmniejszające dotychczasowe i przyszłe skutki kradzieży. W przypadku braku takiej możliwości, osoba okradziona nie miałaby szans poznać rozmiaru szkód, jakie wobec niej poczynili przestępcy, oraz zakresu danych osobowych jakie zostały naruszone.

W ramach projektowanych przepisów określono sposób potwierdzania tożsamości przed rejestracją użytkownika europejskiego portfela tożsamości cyfrowej, zapewnianego przez ministra właściwego do spraw informatyzacji. Przewidziano trzy podstawowe sposoby potwierdzania tożsamości.

Pierwszym sposobem jest wykorzystanie profilu osobistego, który został notyfikowany w Komisji Europejskiej jako środek identyfikacji elektronicznej spełniający wymagania dla wysokiego poziomu bezpieczeństwa[28], dzięki czemu może być bezpośrednio wykorzystany, bez dodatkowych procedur. Zgodnie bowiem z wytycznymi wskazanymi w załączniku do rozporządzenia 2015/1502, w części 2.1.2. zatytułowanej „Sprawdzenie i weryfikacja tożsamości (osoba fizyczna)", dla weryfikacji wysokiego poziomu bezpieczeństwa wskazano w lit. c, że „jeżeli środki identyfikacji elektronicznej są wydawane na podstawie ważnych zgłoszonych środków identyfikacji elektronicznej charakteryzujących się wysokim poziomem bezpieczeństwa i biorąc pod uwagę ryzyko zmiany danych identyfikujących osobę, nie jest konieczne powtarzanie sprawdzania tożsamości oraz procedur weryfikacji…".

Drugim sposobem jest łączone potwierdzenie tożsamości za pomocą profilu zaufanego, jako środka identyfikacji elektronicznej notyfikowanego na średnim poziomie bezpieczeństwa, oraz dodatkowej weryfikacji tożsamości, która będzie realizowana w sposób zgodny z przepisami wykonawczymi, wydanymi na podstawie art. 5 ust. 24 rozporządzenia eIDAS.

Trzeci sposób przewiduje potwierdzenie tożsamości w odpowiednio wyposażonym punkcie potwierdzającym tożsamość, podczas obecności fizycznej, po okazaniu dokumentu stwierdzającego tożsamość i obywatelstwo. Wymaganym będzie okazanie w takim punkcie

[28] Zob. publikacja w Dzienniku Urzędowym Unii Europejskiej C136 z dnia 19 kwietnia 2023 link https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=OJ:C:2023:136:FULL oraz https://ec.europa.eu/digital-building-blocks/sites/spaces/EIDCOMMUNITY/pages/48762251/Overview+of+pre-notified+and+notified+eID+schemes+under+eIDAS

dokumentu stwierdzającego tożsamość i obywatelstwo, który zawiera dowody identyfikacji fotograficznej lub biometrycznej osoby, której tożsamość jest weryfikowana. Wymóg ten jest nawiązaniem do przepisów rozporządzenia 2015/1502, w którym dla potwierdzania tożsamości na wysokim poziomie bezpieczeństwa wymaganym jest, aby – oprócz spełnienia wymogów takich jak przy średnim poziomie bezpieczeństwa oraz weryfikacji autentyczności i ważności dokumentu okazanego dokumentu – dokonano także porównania jednej cechy fizycznej wnioskodawcy, lub większej liczby takich jego cech, z informacjami z wiarygodnego źródła. Wymóg ten spowoduje, że nie będzie możliwe w takim procesie wydanie europejskiego portfela tożsamości cyfrowej osobom, które nie okażą dokumentu zawierającego warstwę elektroniczną, w tym zawierającego co najmniej wbudowany chip RFID[29], w którym przechowuje się dane biometryczne (np. zdjęcie, odciski palców).

Zakłada się, że funkcję punktu potwierdzającego tożsamość będą pełnić wojewodowie, z uwagi na doświadczenie urzędów wojewódzkich w weryfikacji tożsamości cudzoziemców. Projektowane przepisy nie będą narzucały organizacji pracy w tym zakresie, to jest na przykład łączenia załatwiania spraw paszportowych z potwierdzaniem tożsamości dla portfela.

Ponadto przewiduje się, że za zgodą ministra właściwego do spraw informatyzacji, potwierdzanie tożsamości przed wydaniem danych identyfikujących osobę rejestracją użytkownika europejskiego portfela tożsamości cyfrowej będzie mógł pełnić bank krajowy lub organ gminy lub organ miasta na prawach powiatu. Istnienie sieci wyspecjalizowanych punktów potwierdzających tożsamość na wysokim poziomie bezpieczeństwa jest podyktowane potrzebą zapewniania możliwości uzyskania europejskiego portfela tożsamości cyfrowej również rezydentom zamieszkującym Polskę, a nie tylko obywatelom Polski, którzy mają prawo lub obowiązek uzyskania dowodu osobistego z warstwą elektroniczną, i co za tym idzie możliwość samodzielnego potwierdzenia swojej tożsamości za pomocą profilu osobistego. Mimo, że w ramach dodatkowych metod weryfikacji, o których mowa w art. 5 ust. 24 rozporządzenia eIDAS[30], planuje się wykorzystanie zdalnej weryfikacji tożsamości – w szczególności polegającej na porównaniu danych elektronicznych znajdujących się w okazywanych zdalnie dokumentach tożsamości z warstwą elektroniczną, z wizerunkiem wnioskodawcy przekazywanym za pomocą audiowizualnego połączenia nawiązanego z podmiotem profesjonalnie weryfikującym tożsamość – zakłada się, że powinna być także możliwość korzystania również z punktów stacjonarnych. Może być to istotne zwłaszcza w przypadkach, gdyby zdalny sposób dodatkowej weryfikacji tożsamości został tymczasowo zawieszony w związku z potrzebą wprowadzenia uaktualnień, które niezawodnie wykryją nowe sposoby oszustw stosowanych przez przestępców korzystających z oprogramowania fałszującego wizerunek osoby zdalnie potwierdzającej tożsamość.

Projektowane przepisy określają również sposób potwierdzenia tożsamości osoby prawnej przed wydaniem jej danych identyfikujących osobą i rejestracją użytkownika – osoby prawnej w europejskim portfelu tożsamości cyfrowej zapewnianym przez ministra właściwego do spraw informatyzacji.

Zakłada się, że dane identyfikujące osobę prawną, i co z tym idzie portfel osoby prawnej, będą wydawane wyłącznie zarejestrowanym już użytkownikom europejskiego portfela tożsamości cyfrowej, zapewnianego przez ministra właściwego do spraw informatyzacji. Przewiduje się możliwość samodzielnego uzyskania takiego portfela, przez osobę fizyczną uwierzytelnioną łącznie za pomocą swojego europejskiego portfela tożsamości cyfrowej, zapewnianego przez ministra właściwego do spraw informatyzacji, oraz kwalifikowanego elektronicznego

[29] Zgodny z wymaganiami określonymi przez International Civil Aviation Organization w Doc 9303 Machine Readable Travel Documents,

[30] W momencie pisania tego uzasadnienia rozporządzenie wykonawcze Komisji w tej sprawie nie było jeszcze wydane (trwają uzgodnienia)

poświadczenia atrybutów, które będzie poświadczało pełnomocnictwo tej osoby do posługiwania się europejskim portfela tożsamości cyfrowej reprezentowanej osoby prawnej. Przewidziano również możliwość uzyskania wydawanego, przez ministra właściwego do spraw informatyzacji, europejskiego portfela tożsamości cyfrowej osoby prawnej na wniosek osoby prawnej złożony do tego ministra za pomocą specjalnej usługi online. Europejski portfel tożsamości cyfrowej osoby prawnej będzie mogła również uzyskać osoba fizyczna prowadząca działalność gospodarczą, po uwierzytelnieniu za pomocą europejskiego portfela tożsamości cyfrowej wydanego jej jako osoby fizycznej.

Planowane rozwiązanie nie przewiduje odrębnej aplikacji dla uzyskiwania danych identyfikujących osobę prawną i następnie posługiwania się tymi danymi w celu korzystania z usług online przeznaczonych dla osób prawnych, co podyktowane jest następującymi przesłankami:

- przepisy rozporządzenia eIDAS nie wymagają, aby rozwiązania architektoniczne oraz techniczno-organizacyjne dla europejskiego portfela tożsamości cyfrowej, wydanego osobie prawnej, były inne niż dla europejskiego portfela tożsamości cyfrowej, wydanego osobie fizycznej – są one takie same,
- portfel osoby prawnej różni się tylko zestawem danych identyfikujących osobę i co za tym idzie sposobem ich uzyskania,
- z uwagi na istotę narzędzia, jakim jest środek identyfikacji elektronicznej osoby prawnej, należy zabezpieczyć taki środek przed nieuprawnionym przejęciem przez osoby nieupoważnione, jednocześnie możliwość używania tego środka przez osobę upoważnioną, wykorzystującą w tym celu tę samą instancję portfela[31], która posłużyła mu do potwierdzenia swojej tożsamości celem uzyskania danych identyfikujących osobę prawną, którą reprezentuje, jest rozwiązaniem, które zapewni spełnienie powyższego wymagania.

W ramach projektowanych zmian w ustawie z dnia 26 maja 2023 r. o aplikacji mObywatel ustala się również zasady zapewnienia użytkownikom aplikacji mObywatel oraz użytkownikom europejskiego portfela tożsamości cyfrowej funkcjonalności, o której mowa art. 5a ust. 5 lit. g rozporządzenia eIDAS. Zgodnie z tym przepisem europejskie portfele tożsamości cyfrowej muszą oferować wszystkim osobom fizycznym możliwość składania kwalifikowanych podpisów elektronicznych, domyślnie i nieodpłatnie. Mimo, że państwa członkowskie mogą przewidzieć proporcjonalne środki w celu zapewnienia, aby nieodpłatne używanie kwalifikowanych podpisów elektronicznych przez osoby fizyczne było ograniczone do celów innych niż profesjonalne, to i tak obowiązek ten (choć w pomniejszonym zakresie) pozostaje.

Ponieważ w Polsce kwalifikowane podpisy elektroniczne są obecnie dostępne wyłącznie odpłatnie, zapewnienie nieodpłatnych podpisów kwalifikowanych wszystkim użytkownikom portfela w dowolnym celu wiązałoby się z koniecznością dodatkowego sfinansowania takich usług przez państwo. W Polsce państwo wydaje obecnie nieodpłatny podpis osobisty (dostępny dla wszystkich obywateli RP) oraz świadczy powszechnie dostępny (także dla rezydentów) nieopłatny podpis zaufany. Podpisy te, wobec podmiotów publicznych, są równoważne w skutkach prawnych z podpisem własnoręcznym, ale nie są to kwalifikowane podpisy elektroniczne. Ewentualne zmiany w zakresie podpisu zaufanego, które miałby sprawić, aby spełniał on wymogi dla kwalifikowanego podpisu elektronicznego, nie mają sensu, ze względu na konstrukcję tego podpisu elektronicznego (technicznie jest on bowiem pieczęcią elektroniczną ministra właściwego do spraw informatyzacji). Ewentualne, niezbędne zmiany dostosowujące podpis osobisty do wymogów podpisu kwalifikowanego byłyby mniejsze,

[31] W rozumieniu art. 2 pkt 6 rozporządzenia wykonawczego Komisji (UE) 2024/2977

ponieważ konstrukcyjnie jest on taki sam, jak kwalifikowane podpisy elektroniczne. Mimo to, nie doprowadziłoby to do efektu wymaganego na gruncie przepisów rozporządzenia eIDAS. Przepis art. 5a ust. 1 tego rozporządzenia wymaga bowiem zapewnienia europejskiego portfela tożsamości cyfrowej wszystkim osobom fizycznym i prawnym w UE, a nie tylko osobom mającym obywatelstwo polskie. Mając więc na uwadze, że dowód osobisty, a więc i podpis osobisty, wydaje się wyłącznie obywatelowi RP, dostosowanie podpisu osobistego do wymogów kwalifikowanego podpisu elektronicznego również nie jest zasadne.

Z powyższych powodów, aby domyślnie i nieodpłatnie zapewnić wszystkim osobom fizycznym możliwość składania kwalifikowanych podpisów elektronicznych, należałoby wydawać taki podpis w ramach specjalnej usługi publicznej albo zlecić zapewnienie takiego podpisu, za stosowną rekompensatą, kwalifikowanym dostawcom usług zaufania, którzy już obecnie świadczą takie usługi,.

Należy ponadto zaznaczyć, że składanie kwalifikowanego podpisu elektronicznego wymaga użycia kwalifikowanego urządzenia do składania podpisu, a takim urządzeniem nie może być smartfon użytkownika, z uwagi na to, że smartfony nie są obecnie urządzeniami certyfikowanymi w tym kierunku. Mając na uwadze, że część krajowych kwalifikowanych dostawców usług zaufania już obecnie wydaje kwalifikowane podpisy elektroniczne, które wykorzystują kwalifikowane urządzenia do składania podpisu na odległość, należące do tych dostawców usług zaufania (w takim przypadku urządzenie do składania podpisu zapewnia kwalifikowany dostawca), zakłada się, że użytkownicy portfela uzyskają możliwość nieopłatnego składania kwalifikowanego podpisu elektronicznego za pomocą urządzeń do składania podpisu na odległość zapewnianych już obecnie przez krajowych kwalifikowanych dostawców usług zaufania.

Projektowane przepisy zawierają także określenie sposobu, w jaki kwalifikowani dostawcy usług zaufania zostaną upoważnieni do zapewniania użytkownikom portfela nieodpłatnego kwalifikowanego podpisu elektronicznego. Będzie to możliwe na wniosek kwalifikowanego dostawcy usług zaufania, wpisanego do rejestru dostawców usług zaufania. Zakłada się, że wniosek będzie mógł złożyć tylko kwalifikowany dostawca wpisany do wyżej wspomnianego rejestru, z uwagi na to, że tacy kwalifikowani dostawcy pozostają pod nadzorem ministra właściwego do spraw informatyzacji, który jest jednocześnie zobowiązany do zapewnienia europejskiego portfela tożsamości cyfrowej, a zatem jest odpowiedzialny za jego poprawne funkcjonowanie.

Z uwagi na to, że kwalifikowany podpis elektroniczny dla użytkownika portfela ma być zapewniony nieodpłatnie, projektowane przepisy zawierają określenie zasady rekompensowania kwalifikowanym dostawcom usług zaufania kosztów, jakie będą ponosili w związku ze świadczeniem takiej nieodpłatnej usługi. Mając na uwadze potencjalne koszty, jakie trzeba byłoby rekompensować kwalifikowanym dostawcom usług zaufania za świadczenie nieodpłatnych usług, gdyby możliwe byłoby składanie podpisów w każdym celu, ograniczono możliwość składania takich podpisów do celów nieprofesjonalnych. Zakłada się bowiem, że wspólne ponoszenie kosztów przez wszystkich podatników na kwalifikowane podpisy elektroniczne używane nie tylko w celach nieprofesjonalnych, ale również w celu prowadzenia działalności biznesowej przez przedsiębiorców, byłoby nieetyczne, z uwagi na to, że ilość podpisów, jakie potrzebuje złożyć osoba fizyczna w celach nieprofesjonalnych, jest znikoma wobec ilości podpisów, jakie potrzebuje złożyć firma lub osoba fizyczna prowadząca działalność gospodarczą w celach profesjonalnych. Ponadto, warto dodać, że przedsiębiorcy i podmioty publiczne w większości usług publicznych mogą już wykorzystać darmowy podpis zaufany. Przewidziane, na gruncie projektowanej ustawy, świadczenie wyrównawcze dla kwalifikowanych dostawców usług zaufania zostanie w taki sposób skalkulowane, aby zrekompensować ponoszone koszty świadczenia usług (tj. zrekompensować stratę, a nie

zapewnić dochód). Zakłada się, że kwalifikowani dostawcy, którzy zawnioskują o możliwość świadczenia takiego nieopłatnego kwalifikowanego podpisu elektronicznego, osiągną korzyści dzięki większej rozpoznawalności swoich usług i co za tym idzie zwiększeniu sprzedaży świadczonych usług płatnych.

W brzmieniu projektowanych przepisów zdefiniowano cel składania nieodpłatnego kwalifikowanego podpisu elektronicznego „inny niż profesjonalny", mając na uwadze, że termin ten nie został precyzyjnie określony w przepisach rozporządzenia eIDAS. Ponadto, zaproponowano uregulowanie wymagania oznaczania dokumentów elektronicznych opatrzonych takim podpisem w taki sposób, aby możliwe było stwierdzenie, czy podpis ten został użyty w celach „innych niż profesjonalne". Zamierzeniem powyższego jest zapewnienie możliwości odróżnienia przez stronę ufającą, w szczególności klienta podmiotu publicznego lub przedsiębiorcy, czy podmiot ten użył nieodpłatnego kwalifikowanego podpisu elektronicznego zgodnie z jego ustawowym przeznaczeniem. W projekcie nie przewiduje się żadnych sankcji za używanie takiego nieodpłatnego podpisu do celów profesjonalnych. Zakłada się jednakże, że używanie takiego podpisu niezgodnie z jego przeznaczeniem, które będzie dostrzegane przez strony ufające, dzięki wyraźnemu oznaczeniu podpisanego dokumentu, będzie skutkowało utratą zaufania do takiego podpisującego, co w rezultacie będzie pełniło funkcję zapobiegającą takiemu użyciu tego podpisu.

Odrębny pakiet projektowanych przepisów będzie zapewniał rozwiązania, jakie obecnie już z powodzeniem funkcjonują w aplikacji mObywatel, umożliwiając świadczenie podobnych usług także w europejskim portfelu tożsamości cyfrowej, zapewnianym przez ministra właściwego do spraw informatyzacji. Jest to możliwe z uwagi na przepis art. 5a ust. 7 rozporządzenia eIDAS, który wskazuje, że bez uszczerbku dla art. 5f tego rozporządzenia państwa członkowskie mogą przewidzieć, zgodnie z prawem krajowym, dodatkowe funkcje europejskich portfeli tożsamości cyfrowej, w tym interoperacyjność z istniejącymi krajowymi środkami identyfikacji elektronicznej. Przewiduje się bowiem, że europejski portfel tożsamości cyfrowej, wydawany przez ministra właściwego do spraw informatyzacji, oprócz funkcji wymaganych na gruncie rozporządzenia eIDAS, będzie mógł zapewniać użytkownikom również usługi nieprzewidziane w tym rozporządzeniu. Docelowo bowiem nie będzie potrzeby utrzymywania jednocześnie dwóch aplikacji publicznych (tj. aplikacji mObywatel i aplikacji europejskiego portfela tożsamości cyfrowej) zapewniających podobne funkcje – nie tylko ze względu na koszty ich utrzymania, ale też na użytkowników, którzy będą mogli poczuć się zdezorientowani, nie mając pewności, co wybrać. Europejski portfel tożsamości cyfrowej nie będzie w swej istocie stanowić środka do dokonywania płatności, natomiast będzie jedynie stanowić interfejs techniczny dla usług płatniczych. W związku z tym nie wpłynie on na konkurencyjność sektora płatniczego.

W celu zapewnienia funkcjonowania elektronicznych poświadczeń atrybutów, wydawanych do europejskiego portfela tożsamości cyfrowej, które będą ważne wyłącznie w Polsce, powstanie krajowy katalog schematów poświadczania atrybutów, który wzorowany będzie na katalogu schematów prowadzonym przez Komisję Europejską, o którym mowa w art. 8 ust. 3 rozporządzenia wykonawczego Komisji (UE) 2025/1569 z dnia 29 lipca 2025 r. w sprawie ustanowienia zasad stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 w odniesieniu do kwalifikowanych elektronicznych poświadczeń atrybutów oraz elektronicznych poświadczeń atrybutów wydanych przez podmiot sektora publicznego odpowiedzialny za źródło autentyczne lub w jego imieniu (Dz. U. UE. L. z 2025 r. poz. 1569). Na potrzeby usług w europejskim portfelu tożsamości cyfrowej będą pobierane dane wskazane w tym katalogu. Zarówno w katalogu schematów poświadczania atrybutów, prowadzonym przez Komisję Europejską, jak i w planowanym krajowym katalogu schematów poświadczania atrybutów, dokonane zostanie określenie przestrzeni nazw, identyfikatorów atrybutów, opisów

semantycznych każdego atrybutu oraz określenie modelu zaufania i mechanizmów zarządzania stosowanych w ramach schematu, co będzie wynikało z obowiązków nałożonych na gruncie przepisów UE (zob. ww. art. 8 ust. 3 rozporządzenia wykonawczego Komisji (UE) 2025/1569).

VI. Zmiany w z dnia 18 listopada 2020 r. ustawie o doręczeniach elektronicznych

Zmiany mają na celu umożliwienie automatycznego tworzenia ADE dla podmiotów publicznych, które są wpisane już do KPP i mają obowiązek posiadania ADE – ale tylko w przypadku, gdy w KPP będą gromadzone przez ten podmiot wszystkie niezbędne dane wskazane w niniejszej projektowanej zmianie.

Dodatkowo, zmieniono niektóre przepisy, dotyczące podmiotów publicznych, w zakresie odnoszącym się do podawania numeru KPP we wniosku o utworzenia ADE, wpisywania w przypadku tych podmiotów numeru KPP w BAE, czy też możliwości wyszukania tego numeru w wyszukiwarce.

VII. Zmiany w zakresie przepisów ustawy z dnia z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu

Przedmiotowa zmiana spowodowana jest koniecznością doprecyzowania danych identyfikujących klienta w zakresie numeru identyfikacyjnego europejskiego środka identyfikacji elektronicznej, który będzie stanowił odpowiednik serii i numeru dokumentu tożsamości w procesach identyfikacji i weryfikacji tożsamości.

VIII. Pozostałe informacje

Odnosząc się do ewentualnych wątpliwości w zakresie potrzeby dokonania zmian w przepisach sektorowych, które w sposób szczególny dopuszczałyby stosowanie europejskiego portfela tożsamości cyfrowej, przyjęto założenie, że nie ma potrzeby wprowadzania takich przepisów. Należy bowiem wskazać, że każdy europejski portfel tożsamości cyfrowej (w tym także ten, który będzie wydawany w Polsce), musi być zgodnie z art. 5f rozporządzenia eIDAS akceptowany w każdej usłudze online, świadczonej przez podmiot sektora publicznego i w części usług niektórych podmiotów prywatnych.

Podobne założenie przyjęto w projekcie wobec elektronicznych poświadczeń atrybutów wydawanych dla europejskiego portfela tożsamości cyfrowej. Zakłada się bowiem, że nie powinno się w przepisach sektorowych stanowić o możliwości wydawania określonych poświadczeń, o ich zakresach danych, o ich opisach semantycznych, oraz wymaganiach dla takich poświadczeń i mechanizmach zarządzania stosowanych, w celu wydania takich elektronicznych poświadczeń atrybutów. Format, ustalenie zakresu danych i sposób wydawania kwalifikowanych elektronicznych poświadczeń atrybutów oraz elektronicznych poświadczeń atrybutów wydawanych przez podmiot sektora publicznego odpowiedzialny za źródło autentyczne zostały już określone na gruncie przepisów rozporządzenia eIDAS oraz rozporządzenia 2025/1569.

W tym miejscu należy podkreślić, że kwalifikowani dostawcy usług zaufania, wydający elektroniczne poświadczenia atrybutów, są ograniczeni przez wyżej opisane przepisy, stąd też mogą wydawać tylko poświadczenia, które są zgodne ze schematami zgłoszonymi uprzednio do katalogu prowadzonego przez Komisję Europejską i muszą przy tym spełnić wymagania określone w art. 45d rozporządzanie eIDAS. Nie jest wymaganym wprowadzenie żadnych specjalnych przepisów sektorowych, co wynika wprost z art. 45d ust. 3 rozporządzania eIDAS.

Także w odniesieniu do elektronicznych poświadczeń atrybutów, które będą, przez ministra właściwego do spraw informatyzacji, wydawane do – zapewnianego również przez tego ministra – europejskiego portfela tożsamości cyfrowej, mających tylko krajowe znaczenie, zakłada się, że projektowane przepisy wprowadzane w ustawie z dnia 5 września 2016 r.

o usługach zaufania oraz identyfikacji elektronicznej będą wystarczające dla umocowania prawnego tych poświadczeń. Takie poświadczenia będą mogły być wydawane wyłącznie na wniosek zawierający odniesienie do właściwych przepisów, norm lub wytycznych, opisy semantyczne i rodzaje danych każdego atrybutu, który ma być częścią wydawanego elektronicznego poświadczenia atrybutów, a także opis modelu zaufania i mechanizmów zarządzania, stosowanych w celu wydawania wnioskowanego poświadczenia atrybutów, a w tym także mechanizmów unieważnienia oraz opis źródeł informacji, niezbędnych do wydawania takiego elektronicznego poświadczenia atrybutów. Wymaganym będzie zatem przekazanie podobnych informacji, jakie należy przekazać do katalogu schematów poświadczania atrybutów, zgodnie z art. 8 pkt 3 rozporządzenia 2025/1569.

IX. Przepisy przejściowe i końcowe

W projektowanych przepisach przewidziano możliwość uznawania, na poziomie krajowym, europejskiego portfela tożsamości cyfrowej, zapewnianego przez ministra właściwego do spraw informatyzacji, zanim przejdzie on proces certyfikacji, jako środka identyfikacji elektronicznej umożliwiającego uwierzytelniania użytkowników w krajowych usługach publicznych przyłączonych do węzła krajowego identyfikacji elektronicznej, które wymagają uwierzytelnienia użytkownika na średnim poziomie bezpieczeństwa. Przewiduje się, że projektowane przepisy wejdą w życie z dniem 24 grudnia 2026 r., z wyjątkami określonymi w ustawie.

Ponadto zaproponowano późniejsze wejście w życie niektórych przepisów dotyczących KPP.

Projekt ustawy nie jest sprzeczny z prawem Unii Europejskiej.

Projekt ustawy nie wymaga uzyskania opinii, dokonania powiadomienia, konsultacji albo uzgodnienia z właściwymi organami i instytucjami Unii Europejskiej, w tym z Europejskim Bankiem Centralnym, o czym mowa w § 39 uchwały nr 190 Rady Ministrów z dnia 29 października 2013 r. – Regulamin pracy Rady Ministrów (M.P. z 2024 r. poz. 806 oraz 2025 r. poz. 408).

Stosownie do postanowień art. 5 ustawy z dnia 7 lipca 2005 r. o działalności lobbingowej w procesie stanowienia prawa (Dz. U. z 2025 r. poz. 677), projekt zostanie udostępniony w Biuletynie Informacji Publicznej na stronie podmiotowej Ministra Cyfryzacji. Ponadto zgodnie z § 52 ust. 1 uchwały Nr 190 Rady Ministrów z dnia 29 października 2013 r. – Regulamin pracy Rady Ministrów, projekt zostanie udostępniony w Biuletynie Informacji Publicznej na stronie podmiotowej Rządowego Centrum Legislacji w zakładce Rządowy Proces Legislacyjny.