KRAJOWA IZBA
RADCÓW PRAWNYCH

OŚRODEK BADAŃ, STUDIÓW I LEGISLACJI KRAJOWEJ RADY RADCÓW PRAWNYCH

KRAJOWA IZBA RADCÓW PRAWNYCH | ul. Powązkowska 15, 01-797 Warszawa | tel.: 22 300 86 40 | kirp@kirp.pl | NIP 5261043011

Warszawa, dnia 19 marca 2026 r.

Opinia Ośrodka Badań, Studiów i Legislacji Krajowej Rady Radców Prawnych dotycząca projektu ustawy o zmianie ustawy o usługach zaufania oraz identyfikacji elektronicznej oraz niektórych innych ustaw (UC122)

W ocenie autorów, w interesie samorządu radcowskiego konieczne jest wprowadzenie do projektowanych regulacji jednoznacznych rozwiązań prawnych zapewniających pełną ochronę tajemnicy zawodowej radcy prawnego w kontekście stosowania mechanizmów identyfikacji elektronicznej oraz usług zaufania przewidzianych w eIDAS 2.0.

W szczególności należy wprost przewidzieć wyłączenie lub odpowiednie ograniczenie obowiązków wynikających z eIDAS 2.0 w zakresie, w jakim ich realizacja mogłaby prowadzić do naruszenia tajemnicy zawodowej. Regulacje te powinny mieć charakter wyraźny i niepozostawiający wątpliwości interpretacyjnych, tak aby wyeliminować ryzyko kolizji pomiędzy obowiązkami wynikającymi z prawa unijnego a obowiązkami o charakterze zawodowym. Uzasadnieniem dla wprowadzenia powyższego rozwiązania jest szczególny charakter tajemnicy zawodowej radcy prawnego, która – zgodnie z obowiązującymi przepisami – ma charakter bezwzględny oraz nieograniczony w czasie. Tajemnica ta stanowi podstawową gwarancję ochrony praw jednostki oraz warunek prawidłowego funkcjonowania wymiaru sprawiedliwości i obrotu prawnego.

Jednocześnie rozwiązania przewidziane w eIDAS 2.0, w szczególności związane z wykorzystaniem Europejskiego Portfela Tożsamości Cyfrowej oraz mechanizmów udostępniania atrybutów tożsamości, mogą prowadzić do sytuacji, w których:

- dochodzi do przekazywania danych identyfikacyjnych klienta za pośrednictwem podmiotów trzecich,
- zakres ujawnianych informacji wykracza poza minimum niezbędne dla realizacji celu,
- powstaje ryzyko nieuprawnionego dostępu do danych objętych tajemnicą zawodową.
- W tym stanie rzeczy brak jednoznacznych regulacji może prowadzić do powstania realnej kolizji norm prawnych, w której radca prawny będzie zobowiązany jednocześnie do realizacji obowiązków identyfikacyjnych wynikających z eIDAS 2.0 oraz do bezwzględnego zachowania tajemnicy zawodowej.
- W celu uniknięcia takiej sytuacji ustawodawca powinien wprowadzić przepisy szczególne, które:
- jednoznacznie potwierdzą pierwszeństwo obowiązku zachowania tajemnicy zawodowej w przypadku kolizji z obowiązkami wynikającymi z regulacji dotyczących identyfikacji elektronicznej,
- ograniczą zakres danych, które mogą być pozyskiwane lub przetwarzane przez radców prawnych przy wykorzystaniu narzędzi eIDAS 2.0 do minimum niezbędnego,
- wyłączą możliwość nakładania na radców prawnych obowiązków ujawniania informacji objętych tajemnicą zawodową w ramach mechanizmów identyfikacyjnych lub usług zaufania.

Wprowadzenie powyższych rozwiązań jest konieczne dla zapewnienia spójności systemu prawnego oraz zagwarantowania, że rozwój narzędzi identyfikacji cyfrowej nie doprowadzi do osłabienia standardów ochrony prawnej jednostki ani do naruszenia istoty zawodu radcy prawnego jako zawodu zaufania publicznego.

1.1 Status radcy prawnego jako podmiotu zaufania w systemie eIDAS 2.0

W ocenie autorów, w interesie samorządu radcowskiego konieczne jest rozważenie wprowadzenia do krajowych przepisów implementujących eIDAS 2.0 rozwiązań

przyznających radcom prawnym szczególną rolę w systemie identyfikacji elektronicznej oraz obiegu atrybutów tożsamości.

W szczególności należy rozważyć normatywne ukształtowanie statusu radcy prawnego jako podmiotu zaufania publicznego uczestniczącego w procesie weryfikacji określonych atrybutów tożsamości lub uprawnień, w zakresie związanym z wykonywaniem zawodu. Rozwiązanie to mogłoby obejmować w szczególności możliwość potwierdzania przez radców prawnych określonych cech lub statusów prawnych (np. umocowania, reprezentacji, spełnienia określonych przesłanek formalnych), które następnie mogłyby być wykorzystywane w ramach ekosystemu eIDAS 2.0.

Uzasadnieniem dla powyższego postulatu jest szczególna pozycja radcy prawnego jako zawodu zaufania publicznego, którego istotą jest zapewnienie bezpieczeństwa obrotu prawnego oraz ochrona praw jednostki. Włączenie radców prawnych w system weryfikacji atrybutów mogłoby przyczynić się do zwiększenia wiarygodności danych wykorzystywanych w obrocie cyfrowym oraz ograniczenia ryzyk związanych z błędną lub niepełną identyfikacją.

Jednocześnie brak odpowiednich regulacji w tym zakresie może prowadzić do marginalizacji roli profesjonalnych pełnomocników w procesach identyfikacyjnych, które, w świetle eIDAS 2.0, mogą być w coraz większym stopniu realizowane przez podmioty technologiczne lub dostawców usług cyfrowych. Taka sytuacja mogłaby skutkować osłabieniem gwarancji prawnych oraz przeniesieniem kluczowych funkcji związanych z weryfikacją tożsamości i uprawnień poza sferę zawodów zaufania publicznego. W związku z powyższym ustawodawca powinien rozważyć wprowadzenie przepisów, które:

- umożliwią radcom prawnym uczestnictwo w systemach potwierdzania atrybutów tożsamości lub uprawnień w ramach eIDAS 2.0,
- określą zakres i skutki prawne takich potwierdzeń,
- zapewnią odpowiedni poziom zaufania i odpowiedzialności związany z wykonywaniem tych funkcji,
- zagwarantują, że udział radców prawnych w tym systemie będzie zgodny z zasadami wykonywania zawodu, w tym obowiązkiem zachowania tajemnicy zawodowej.

Wprowadzenie powyższych rozwiązań mogłoby przyczynić się do lepszego wykorzystania potencjału zawodów zaufania publicznego w procesie cyfryzacji obrotu prawnego oraz zapewnienia wyższego poziomu bezpieczeństwa i wiarygodności mechanizmów identyfikacji elektronicznej.

1.2 Europejski Portfel Tożsamości Cyfrowej a relacja pełnomocnik–klient

W ocenie autorów, w interesie samorządu radcowskiego konieczne jest jednoznaczne uregulowanie w przepisach krajowych zasad korzystania przez radców prawnych z danych pochodzących z Europejskiego Portfela Tożsamości Cyfrowej w relacji pełnomocnik–klient.

W szczególności ustawodawca powinien w sposób wyraźny określić dopuszczalny zakres wykorzystania danych i atrybutów tożsamości udostępnianych przez klienta za pośrednictwem EU Wallet, tak aby wyeliminować niepewność prawną oraz zapewnić zgodność praktyki zawodowej z obowiązującymi standardami ochrony danych i tajemnicy zawodowej. Regulacja ta powinna w szczególności rozstrzygać:

- czy i na jakich zasadach radca prawny może korzystać z danych udostępnionych przez klienta za pośrednictwem Europejskiego Portfela Tożsamości Cyfrowej,
- w jakim zakresie dopuszczalne jest utrwalanie i przechowywanie tych danych w dokumentacji prowadzonej sprawy,
- czy oraz na jakich warunkach dane i atrybuty pozyskane z EU Wallet mogą być wykorzystywane jako materiał dowodowy w postępowaniach sądowych lub administracyjnych.

Brak jednoznacznych regulacji w powyższym zakresie może prowadzić do istotnych wątpliwości praktycznych, w szczególności:

- czy dane pozyskane z EU Wallet mogą być traktowane jako równoważne tradycyjnym dokumentom,
- czy ich wykorzystanie nie narusza zasady minimalizacji danych oraz obowiązku ograniczenia celu przetwarzania,
- jakie są granice odpowiedzialności radcy prawnego za prawidłowość i aktualność tych danych.

W związku z powyższym konieczne jest wprowadzenie przepisów, które:

- określą status prawny danych i atrybutów pochodzących z Europejskiego Portfela Tożsamości Cyfrowej w obrocie prawnym,
- jednoznacznie uregulują dopuszczalność ich wykorzystania przez profesjonalnych pełnomocników,
- wskażą zasady ich przechowywania, w tym okresy retencji oraz warunki zabezpieczenia,
- określą ich wartość dowodową oraz warunki dopuszczalności jako środka dowodowego.
- Jednocześnie regulacje te powinny zapewniać pełną zgodność z obowiązkiem zachowania tajemnicy zawodowej oraz przepisami o ochronie danych osobowych, a także uwzględniać specyfikę relacji pełnomocnik–klient, w której szczególne znaczenie ma zaufanie oraz poufność przekazywanych informacji.

Wprowadzenie powyższych rozwiązań jest niezbędne dla zapewnienia pewności prawa oraz umożliwienia bezpiecznego i efektywnego wykorzystania Europejskiego Portfela Tożsamości Cyfrowej w praktyce świadczenia usług prawnych.

1.3 Odpowiedzialność za błędną identyfikację

W ocenie autorów, w interesie samorządu radcowskiego konieczne jest jednoznaczne i wyczerpujące uregulowanie zasad odpowiedzialności za błędy identyfikacji elektronicznej w ramach systemu eIDAS 2.0, w szczególności w kontekście wykorzystania Europejskiego Portfela Tożsamości Cyfrowej.

W szczególności ustawodawca powinien w sposób jednoznaczny określić podział odpowiedzialności pomiędzy dostawcami usług identyfikacji elektronicznej, użytkownikami (posiadaczami portfela) oraz profesjonalnymi uczestnikami obrotu, w tym radcami prawnymi. Brak takich regulacji prowadzić będzie do istotnej niepewności prawnej oraz ryzyka przerzucania odpowiedzialności na najsłabsze ogniwa systemu. Obecnie projektowane rozwiązania mogą prowadzić do sytuacji, w których:

- dane identyfikacyjne lub atrybuty okażą się nieaktualne, niepełne lub nieprawdziwe,
- dojdzie do nieuprawnionego użycia środków identyfikacji elektronicznej,
- błędna identyfikacja stanie się podstawą czynności prawnej lub procesowej.

W takich przypadkach brak jasnych zasad odpowiedzialności może prowadzić do powstania sporów co do tego, czy odpowiedzialność ponosi:

- dostawca usługi identyfikacji (np. podmiot wydający portfel lub potwierdzający atrybuty),
- użytkownik posługujący się środkiem identyfikacji,
- czy też profesjonalny pełnomocnik, który polegał na uzyskanych danych.

W związku z powyższym konieczne jest wprowadzenie przepisów, które:

- jednoznacznie przypiszą odpowiedzialność za prawidłowość danych identyfikacyjnych i atrybutów podmiotom je wydającym lub potwierdzającym,
- określą zakres odpowiedzialności użytkownika za posługiwanie się środkami identyfikacji elektronicznej, w tym w przypadku ich utraty lub nieuprawnionego użycia,
- wyraźnie wyłączą lub ograniczą odpowiedzialność profesjonalnych pełnomocników w sytuacji, gdy działali oni w zaufaniu do środków identyfikacji spełniających wymogi eIDAS 2.0,
- wprowadzą domniemania prawne dotyczące wiarygodności danych pochodzących z kwalifikowanych środków identyfikacji, przy jednoczesnym określeniu przesłanek ich obalenia.

Należy podkreślić, że bez wprowadzenia powyższych rozwiązań istnieje realne ryzyko przeniesienia ciężaru odpowiedzialności na uczestników obrotu prawnego, którzy nie mają faktycznego wpływu na proces generowania i weryfikacji danych identyfikacyjnych. Taka sytuacja byłaby sprzeczna z zasadą zaufania do państwa i stanowionego prawa oraz mogłaby prowadzić do ograniczenia wykorzystania narzędzi eIDAS 2.0 w praktyce.

Wprowadzenie jasnych i przewidywalnych zasad odpowiedzialności jest zatem warunkiem koniecznym dla zapewnienia bezpieczeństwa obrotu prawnego oraz efektywnego funkcjonowania systemu identyfikacji elektronicznej.

1.4 Interoperacyjność rozwiązań eIDAS 2.0 a praktyka krajowa

W ocenie autorów, w interesie samorządu radcowskiego konieczne jest zapewnienie pełnej interoperacyjności rozwiązań przewidzianych w eIDAS 2.0 z krajowym porządkiem prawnym,

w szczególności z regulacjami proceduralnymi oraz ukształtowaną praktyką stosowania prawa.

W szczególności ustawodawca powinien jednoznacznie uregulować sposób funkcjonowania środków identyfikacji elektronicznej oraz atrybutów tożsamości w krajowych postępowaniach sądowych i administracyjnych, tak aby zapewnić ich rzeczywistą użyteczność w obrocie prawnym. Regulacje te powinny w szczególności obejmować:

1. postępowanie cywilne – poprzez jednoznaczne określenie:
    - statusu dowodowego danych i atrybutów pochodzących z Europejskiego Portfela Tożsamości Cyfrowej,
    - zasad ich dopuszczalności jako środka dowodowego,
    - relacji pomiędzy dokumentami elektronicznymi generowanymi w systemie eIDAS 2.0 a tradycyjnymi dokumentami prywatnymi i urzędowymi,
2. postępowania administracyjne – poprzez:
    - zapewnienie możliwości skutecznego posługiwania się środkami identyfikacji elektronicznej w kontaktach z organami administracji,
    - określenie zasad uwzględniania atrybutów tożsamości przy załatwianiu spraw administracyjnych,
    - doprecyzowanie wymogów formalnych dla czynności dokonywanych przy użyciu EU Wallet,
3. praktykę sądową – poprzez:
    - dostosowanie systemów teleinformatycznych sądów do obsługi środków identyfikacji elektronicznej zgodnych z eIDAS 2.0,
    - wypracowanie jednolitych standardów akceptacji danych i atrybutów pochodzących z EU Wallet,
    - zapewnienie spójności orzecznictwa w zakresie oceny wiarygodności takich danych.

Brak odpowiednich regulacji w powyższym zakresie może prowadzić do sytuacji, w której rozwiązania eIDAS 2.0 – mimo formalnego obowiązywania – nie będą w pełni wykorzystywane w praktyce krajowej, co podważy ich funkcjonalność oraz ograniczy korzyści wynikające z cyfryzacji obrotu prawnego.

W związku z powyższym konieczne jest wprowadzenie przepisów zapewniających spójność pomiędzy regulacjami unijnymi a krajowymi procedurami, w szczególności poprzez:

- jednoznaczne określenie skutków prawnych czynności dokonywanych przy wykorzystaniu środków identyfikacji elektronicznej,
- dostosowanie przepisów proceduralnych do nowych form identyfikacji i dokumentowania czynności prawnych,
- zapewnienie jednolitego stosowania prawa przez sądy i organy administracji.

Zapewnienie interoperacyjności na poziomie normatywnym i praktycznym stanowi warunek konieczny dla skutecznego wdrożenia eIDAS 2.0 oraz dla zapewnienia, że nowe rozwiązania będą realnie wspierać, a nie komplikować, funkcjonowanie obrotu prawnego.

1.5 Interoperacyjność rozwiązań eIDAS 2.0 a praktyka krajowa

W ocenie autorów, w interesie samorządu radcowskiego konieczne jest jednoznaczne doprecyzowanie relacji pomiędzy regulacjami eIDAS 2.0 a przepisami o ochronie danych osobowych, w szczególności w zakresie przetwarzania danych pochodzących z Europejskiego Portfela Tożsamości Cyfrowej.

W szczególności ustawodawca powinien w sposób wyraźny określić podstawy prawne przetwarzania danych i atrybutów tożsamości udostępnianych za pośrednictwem EU Wallet, z uwzględnieniem specyfiki relacji pomiędzy użytkownikiem, dostawcą usługi oraz podmiotem korzystającym z danych (w tym profesjonalnym pełnomocnikiem). Brak takiego doprecyzowania może prowadzić do niepewności co do legalności przetwarzania danych oraz ryzyka naruszenia przepisów o ochronie danych osobowych.

Jednocześnie konieczne jest wprowadzenie jednoznacznych regulacji gwarantujących stosowanie zasady minimalizacji danych, zgodnie z którą przetwarzane powinny być wyłącznie dane niezbędne dla realizacji określonego celu. W kontekście eIDAS 2.0 oznacza to w szczególności zapewnienie, że mechanizmy udostępniania atrybutów tożsamości będą ograniczone do zakresu adekwatnego do konkretnej czynności prawnej lub faktycznej.

Ponadto ustawodawca powinien zapewnić pełną zgodność rozwiązań eIDAS 2.0 z zasadą kontroli danych przez użytkownika, stanowiącą jeden z fundamentów systemu ochrony danych osobowych. Oznacza to konieczność zagwarantowania, że:

- użytkownik będzie miał realny wpływ na zakres udostępnianych danych i atrybutów,
- udostępnianie danych będzie następowało w sposób świadomy i dobrowolny,
- użytkownik będzie posiadał możliwość śledzenia oraz weryfikacji, komu i w jakim zakresie dane zostały udostępnione.

Wskazane powyżej postulaty znajdują uzasadnienie w podstawowych zasadach przetwarzania danych osobowych, takich jak zasada legalności, minimalizacji danych oraz zapewnienia odpowiedniego poziomu bezpieczeństwa przetwarzania. Brak ich odpowiedniego odzwierciedlenia w regulacjach krajowych może prowadzić do powstania napięć pomiędzy systemem identyfikacji elektronicznej a systemem ochrony danych osobowych. W związku z powyższym konieczne jest zapewnienie spójności pomiędzy eIDAS 2.0 a RODO na poziomie normatywnym i praktycznym, w szczególności poprzez:

- doprecyzowanie podstaw przetwarzania danych w różnych modelach wykorzystania EU Wallet,
- wprowadzenie mechanizmów technicznych i prawnych ograniczających zakres przetwarzanych danych,
- zapewnienie skutecznych instrumentów kontroli po stronie użytkownika.

Zapewnienie tej spójności stanowi warunek konieczny dla budowy zaufania do systemu identyfikacji cyfrowej oraz dla jego efektywnego i zgodnego z prawem wykorzystania w praktyce obrotu prawnego.

2 Wnioski

Regulacje eIDAS 2.0 wprowadzają fundamentalną zmianę w sposobie identyfikacji i komunikacji prawnej w środowisku cyfrowym, tworząc podstawy europejskiej infrastruktury zaufania. Zmiana modelu identyfikacji (z dokumentowego na atrybutowy) oraz wdrożenie Europejskiego Portfela Tożsamości Cyfrowej będą miały bezpośredni

wpływ na sposób wykonywania zawodu radcy prawnego oraz funkcjonowanie obrotu prawnego.

Z perspektywy samorządu radcowskiego konieczne jest podjęcie pilnych i skoordynowanych działań przygotowawczych – w szczególności w obszarze regulacyjnym, edukacyjnym i technologicznym – tak aby zapewnić bezpieczne i zgodne z prawem wykorzystanie nowych narzędzi w praktyce zawodowej.

Jednocześnie projektowane regulacje wymagają istotnych doprecyzowań na poziomie ustawowym. Kluczowe znaczenie ma w szczególności:

- zapewnienie pełnej ochrony tajemnicy zawodowej w kontekście mechanizmów identyfikacji elektronicznej,
- jednoznaczne określenie zasad odpowiedzialności za błędną identyfikację,
- uregulowanie wykorzystania danych z Europejskiego Portfela Tożsamości Cyfrowej
  w relacji pełnomocnik–klient,
- zagwarantowanie spójności rozwiązań eIDAS 2.0 z krajowymi procedurami oraz przepisami o ochronie danych osobowych.

Bez wprowadzenia powyższych rozwiązań istnieje ryzyko powstania niepewności prawnej oraz osłabienia standardów ochrony uczestników obrotu. Prawidłowe wdrożenie eIDAS 2.0 powinno zatem opierać się na równowadze pomiędzy rozwojem usług cyfrowych a zachowaniem fundamentalnych zasad wykonywania zawodu radcy prawnego oraz ochrony praw jednostki.

3 Autorzy

dr inż. Rafał Tomasz Prabucki – doktor nauk prawnych i inżynier. Członek Społecznego Zespołu Ekspertów przy Prezesie Urzędu Ochrony Danych Osobowych. Auditor wiodący ISO/IEC 27001, BCMS ISO 22301 oraz ISO/IEC 42001/2023. Posiadacz tytułu Certified in Cybersecurity (CC) wydanego przez $(ISC)^2$. Adiunkt na Uniwersytecie Śląskim. Członek CYBER SCIENCE i SABI. Założyciel LegalHackers Katowice. Asystent w zakończonych projektach dotyczących wykorzystania przełomowych technik w przemyśle: MAS4AI na Uniwersytecie Śląskim i SHOP4CF na Uniwersytecie Opolskim. Alumn stypendiów w Polsce, Hiszpanii i Niemczech.

mgr Mateusz Jakubik – Prawnik z doświadczeniem łączącym aspekty prawne z IT. Zawodowo związany z Bonnier Business Polska (CISO), InfinityLawTech (Partner) oraz ODO Szkolenia (CIO). Jest certyfikowanym Auditorem wiodącym systemów zarządzania bezpieczeństwem informacji (ISO/IEC 27001), ciągłością działania (ISO 22301) oraz sztuczną inteligencją (ISO/IEC 42001). Doświadczenie zdobywał m.in. w jednej z renomowanych warszawskich kancelarii specjalizującej się w RODO oraz w spółce Skarbu Państwa z sektora energetycznego. Na co dzień pełni funkcję Inspektora Ochrony Danych i dzieli się wiedzą jako wykładowca akademicki, kładąc nacisk na praktyczne zastosowanie prawa w środowisku cyfrowym.