KRAJOWA IZBA
RADCÓW PRAWNYCH

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

L.dz. 653/2026 Warszawa, dnia 30 czerwca 2026 roku

Szanowna Pani
P.

W odpowiedzi na wniosek z dnia 10 kwietnia 2026 r. (data wpływu 20.04.2026r.), dotyczący wyjaśnienia zagadnienia z zasad etyki i wykonywania zawodu radcy prawnego w zakresie dopuszczalności i bezpieczeństwa posługiwania się przez radcę prawnego zatrudnionego w spółce prawa handlowego kwalifikowanym podpisem elektronicznym (np. „Szafir") przy użyciu sprzętu służbowego pracodawcy, nad którym radca prawny nie ma pełnej kontroli technicznej i administracyjnej, Komisja Etyki i Wykonywania Zawodu Krajowej Rady Radców Prawnych, mając na uwadze przedstawiony we wniosku stan faktyczny oraz uzasadnienie pytań, informuje, że:

1) Kwalifikowany podpis elektroniczny oparty na infrastrukturze klucza publicznego (PKI), taki jak podpis kartowy (karta kryptograficzna + czytnik) lub chmurowy (np. mSzafir, SimplySign), posiada wbudowane mechanizmy ochrony klucza prywatnego, które są niezależne od środowiska systemu operacyjnego urządzenia, na którym podpis jest stosowany. Klucz prywatny, stanowiący rdzeń podpisu kwalifikowanego, nie opuszcza karty kryptograficznej lub bezpiecznego środowiska chmurowego dostawcy certyfikacyjnego.

2) Samo korzystanie przez radcę prawnego z kwalifikowanego podpisu elektronicznego na sprzęcie służbowym pracodawcy – bez pełnych uprawnień administratorskich na tym urządzeniu – nie stanowi samo w sobie naruszenia zasad etyki zawodowej ani standardów należytej staranności, o ile radca prawny zapewnia wyłączną kontrolę nad elementami autoryzacji podpisu (karta kryptograficzna, PIN, aplikacja mobilna) i stosuje właściwe praktyki bezpieczeństwa.

3) W każdym przypadku radca prawny zobowiązany jest do dokonania samodzielnej oceny ryzyka naruszenia obowiązujących zasad etyki zawodowej, ze szczególnym uwzględnieniem faktycznych warunków techniczno-organizacyjnych środowiska, w którym podpis jest stosowany.

Wyjaśniając powyższe, Komisja wskazuje, co następuje:

I. Ocena zagadnienia będącego przedmiotem odpowiedzi Komisji została dokonana z uwzględnieniem:

a) ustawy z dnia 6 lipca 1982 r. o radcach prawnych (t.j. Dz.U. z 2024 r., poz. 499 ze zm.), zwanej dalej *„ustawą o radcach prawnych"* lub *„u.r.p."*,

b) Kodeksu Etyki Radcy Prawnego (w brzmieniu stanowiącym załącznik do Uchwały nr 884/XI/2023 Prezydium Krajowej Rady Radców Prawnych z dnia 7 lutego 2023r. w sprawie ogłoszenia tekstu jednolitego Kodeksu Etyki Radcy Prawnego), zwanego dalej *„Kodeksem Etyki Radcy Prawnego”* lub *„KERP”*,

c) Regulaminu wykonywania zawodu radcy prawnego (w brzmieniu stanowiącym załącznik do Uchwały nr 917/XI/2023 Prezydium Krajowej Rady Radców Prawnych z dnia 8 marca 2023 r. w sprawie ogłoszenia tekstu jednolitego Regulaminu wykonywania zawodu radcy prawnego), zwanego dalej *„Regulaminem”*,

d) Rozporządzenia 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 (eIDAS), zwanego dalej „*rozporządzeniem eIDAS*”, w szczególności art. 25 i 26,

e) ustawy z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej (t.j. Dz.U. z 2021 r., poz. 1797 ze zm.).

II. Uzasadnienie stanowiska Komisji w przedstawionej sprawie

A. Techniczna architektura kwalifikowanego podpisu elektronicznego

1. Kwalifikowany podpis elektroniczny, w rozumieniu art. 3 pkt 12 rozporządzenia eIDAS, stanowi zaawansowany podpis elektroniczny złożony za pomocą kwalifikowanego urządzenia do składania podpisu elektronicznego, oparty na kwalifikowanym certyfikacie podpisu elektronicznego. Jego zasadniczą cechą jest to, że klucz prywatny podpisującego jest generowany i przechowywany w bezpiecznym urządzeniu kryptograficznym (karta kryptograficzna zgodna z FIPS 140-2 lub CC EAL4+), które projektowo uniemożliwia eksport klucza. Architektura ta oznacza, że klucz prywatny nie istnieje poza kartą w żadnej odczytywalnej postaci.

2. W praktyce funkcjonujących na rynku polskim rozwiązań podpisu kwalifikowanego wyróżnić należy dwa modele:

a) model kartowy – klucz prywatny zapisany na fizycznej karcie kryptograficznej; podpisanie dokumentu wymaga fizycznej obecności karty w czytniku podłączonym do urządzenia oraz wprowadzenia kodu PIN przez radcę prawnego;

b) model chmurowy (np. mSzafir, SimplySign) – klucz prywatny przechowywany w infrastrukturze kryptograficznej dostawcy certyfikacyjnego (HSM – sprzętowy moduł bezpieczeństwa); każdorazowe podpisanie wymaga aktywnej autoryzacji ze strony radcy prawnego poprzez

dedykowaną aplikację mobilną na jego osobistym urządzeniu lub weryfikację kodem SMS.

3. W obu modelach uprawnienia administracyjne pracowników działu IT pracodawcy na urządzeniu służbowym (komputerze) nie dają dostępu do klucza prywatnego ani nie umożliwiają złożenia podpisu bez wiedzy i aktywnego udziału radcy prawnego. Środowisko systemowe komputera i środowisko kryptograficzne podpisu są od siebie projektowo i technicznie odseparowane.

B. Ocena w świetle zasad etyki radcy prawnego

1. Obowiązek zachowania należytej staranności (art. 3 ust. 2 u.r.p., art. 12 ust. 1 KERP) oraz obowiązek ochrony tajemnicy zawodowej (art. 3 ust. 3-5 u.r.p., art. 9, art. 15 i nast. KERP) należy interpretować z uwzględnieniem rzeczywistych właściwości stosowanego narzędzia technicznego. Przy prawidłowym korzystaniu z kwalifikowanego podpisu elektronicznego w modelu kartowym lub chmurowym, faktyczne ryzyko nieautoryzowanego złożenia podpisu przez osoby trzecie (w tym pracowników IT pracodawcy) jest wyeliminowane przez architekturę systemu, a nie jedynie zredukowane przez procedury organizacyjne.
2. Zasada niezależności zawodowej radcy prawnego (art. 7 KERP) nie stoi w sprzeczności z korzystaniem z kwalifikowanego podpisu elektronicznego w infrastrukturze pracodawcy, jeśli radca prawny zachowuje wyłączną kontrolę nad elementami autoryzacji: kartą kryptograficzną, kodem PIN oraz urządzeniem mobilnym służącym do autoryzacji chmurowej.
3. Domniemanie autentyczności złożonego podpisu wynikające z art. 25 rozporządzenia eIDAS ma charakter wzruszalny. Ryzyko przypisania radcy prawnemu skutków prawnych czynności dokonanych bez jego wiedzy, przy prawidłowym korzystaniu z podpisu kwalifikowanego, jest porównywalne z ryzykiem właściwym dla innych narzędzi i dokumentów służbowych – w szczególności analogicznym do ryzyka wynikającego z pozostawienia przez radcę prawnego niezabezpieczonych dokumentów papierowych lub dostępu osób nieuprawnionych do jego komputera z niezablokowaną sesją.
4. Korzystanie z kwalifikowanego podpisu elektronicznego dla dokumentów wewnętrznych pracodawcy, które nie wymagają z mocy prawa zastosowania tej formy, nie jest samo w sobie działaniem nieproporcjonalnym ani naruszającym KERP. Ocena zasadności stosowania tej formy należy do pracodawcy określającego zasady wewnętrznego obiegu dokumentów, zaś rolą radcy prawnego jest zapewnienie, że sposób korzystania z podpisu odpowiada wymogom etyki zawodowej.

C. Realne ryzyka i minimalne standardy staranności

1. Komisja wskazuje, że realne ryzyka związane z korzystaniem z kwalifikowanego podpisu elektronicznego na sprzęcie służbowym nie wynikają z braku uprawnień administratorskich radcy prawnego na urządzeniu, lecz z zachowań niezgodnych z wymogami należytej staranności zawodowej, w szczególności:

   - pozostawienia karty kryptograficznej w czytniku bez nadzoru przy niezablokowanej sesji na urządzeniu;

   - udostępnienia kodu PIN osobom trzecim;

   - korzystania z niezabezpieczonego urządzenia mobilnego służącego do autoryzacji chmurowej;

   - niepodejmowania weryfikacji treści dokumentu przed złożeniem podpisu (ryzyko ataku polegającego na podstawieniu dokumentu).

2. Minimalne standardy należytej staranności przy korzystaniu z kwalifikowanego podpisu elektronicznego w środowisku służbowym obejmują:

   - przechowywanie karty kryptograficznej wyłącznie przez radcę prawnego i jej wyjmowanie z czytnika po zakończeniu czynności podpisywania;

   - zachowanie poufności kodu PIN i jego nieudostępnianie jakimkolwiek osobom trzecim;

   - każdorazową weryfikację treści i integralności dokumentu przed złożeniem podpisu;

   - zabezpieczenie urządzenia mobilnego używanego do autoryzacji w modelu chmurowym.

D. Prawo odmowy stosowania podpisu w warunkach zagrożenia

1. Zasada niezależności zawodowej (art. 7 KERP) przyznaje radcy prawnemu prawo, a w sytuacji realnego zagrożenia tajemnicy zawodowej – obowiązek odmowy stosowania kwalifikowanego podpisu elektronicznego, jeśli pracodawca wymaga korzystania z niego w warunkach faktycznie uniemożliwiających zachowanie wyłącznej kontroli nad elementami autoryzacji (np. wymagając udostępnienia PIN-u administratorowi lub przechowywania karty w miejscu dostępnym dla innych osób). Odmowa taka mieści się w granicach odpowiedzialnej, tj. zgodnej z przepisami prawa i zasadami etyki (wymaganej) postawy zawodowej radcy prawnego i nie stanowi naruszenia obowiązków pracowniczych.

2. Komisja podkreśla, że polecenie pracodawcy nie zwalnia radcy prawnego z odpowiedzialności za naruszenie zasad etyki zawodowej. W przypadku konfliktu pomiędzy wymaganiami pracodawcy a standardami KERP, radca prawny powinien niezwłocznie zgłosić zastrzeżenia pracodawcy na piśmie, wskazując na konkretne zagrożenia wynikające z proponowanego sposobu

korzystania z podpisu (§ 9 ust. 2 Regulaminu; zob. także art. 40 KERP dot. regulacji wewnętrznych).

III. Wnioski końcowe

1. Korzystanie przez radcę prawnego zatrudnionego w spółce prawa handlowego z kwalifikowanego podpisu elektronicznego (kartowego lub chmurowego) na sprzęcie służbowym pracodawcy, nad którym radca prawny nie posiada pełnych uprawnień administracyjnych, jest co do zasady dopuszczalne i nie narusza przepisów KERP, jeżeli radca prawny zachowuje wyłączną kontrolę nad elementami autoryzacji podpisu.
2. Brak uprawnień administratorskich na urządzeniu służbowym nie jest tożsamy z brakiem kontroli nad kwalifikowanym podpisem elektronicznym ze względu na architektoniczną separację środowiska systemowego i środowiska kryptograficznego podpisu.
3. Radca prawny jest zobowiązany do zachowania standardów staranności właściwych dla ochrony klucza kryptograficznego i elementów autoryzacji, analogicznie jak do zachowania należytej staranności przy ochronie innych narzędzi i dokumentów zawodowych.
4. W każdym przypadku konieczna jest indywidualna ocena warunków faktycznych korzystania z podpisu i radca prawny zobowiązany jest do odmowy stosowania podpisu kwalifikowanego, jeżeli rzeczywiste warunki techniczne lub organizacyjne narzucone przez pracodawcę uniemożliwiają mu zachowanie wyłącznej kontroli nad elementami autoryzacji.

Komisja Etyki i Wykonywania Zawodu Krajowej Rady Radców Prawnych w składzie:
r.pr. dr Katarzyna Palka-Bartoszek (przewodnicząca)
r.pr. Jolanta Czepe
r.pr. Andrzej Kadzik
r.pr. Agata Gutowska,
r.pr. Karolina Pukańska-Dura
r.pr. Rafał Rybnik (opracowanie)
r.pr. Grzegorz Wyszogrodzki
r.pr. Jacek Zieleziński

Przewodnicząca
Komisji Etyki i Wykonywania Zawodu
Krajowej Rady Radców Prawnych
r.pr. dr Katarzyna Palka-Bartoszek