USŁUGI ZAUFANIA ORAZ IDENTYFIKACJA ELEKTRONICZNA

Komentarz

redakcja naukowa
Agnieszka Skóra, Błażej Kwiatek

Marcin Adamczyk, Paulina Bieś-Srokosz, Wojciech Cieślak
Magdalena Ciorgoń-Urbańska, Maciej Górtowski
Mirosław Karpiuk, Błażej Kwiatek, Grzegorz Makarow
Remigiusz Mazur, Agnieszka Skóra, Arkadiusz Talik
Karol Wach, Dawid Ziółkowski

KOMENTARZE PRAKTYCZNE

Wolters Kluwer

USŁUGI ZAUFANIA ORAZ IDENTYFIKACJA ELEKTRONICZNA

Komentarz

redakcja naukowa
Agnieszka Skóra, Błażej Kwiatek

Marcin Adamczyk, Paulina Bieś-Srokosz, Wojciech Cieślak
Magdalena Ciorgoń-Urbańska, Maciej Górtowski
Mirosław Karpiuk, Błażej Kwiatek, Grzegorz Makarow
Remigiusz Mazur, Agnieszka Skóra, Arkadiusz Talik
Karol Wach, Dawid Ziółkowski

KOMENTARZE PRAKTYCZNE

Wolters Kluwer

WARSZAWA 2024

Stan prawny na 6 stycznia 2024 r.

Recenzent
Dr hab. Grzegorz Sibiga, prof. INP PAN

Wydawca
Małgorzata Stańczak

Redaktor prowadzący
Joanna Tchorek

Opracowanie redakcyjne
Agnieszka Witczak

Projekt okładek serii
Wojtek Janikowski, Przemek Dębowski

Komentarze do poszczególnych artykułów napisali:
Marcin Adamczyk – art. 10–12, 31–33, 36–39b
Marcin Adamczyk, Agnieszka Skóra – art. 2, 3, 7, 9
Paulina Bieś-Srokosz, Remigiusz Mazur, Arkadiusz Talik – art. 46–49
Wojciech Cieślak, Maciej Górtowski – art. 40–45
Magdalena Ciorgoń-Urbańska – art. 27–30, 39g, 39h, 131–133, 135–137, 139
Mirosław Karpiuk – art. 35
Błażej Kwiatek – art. 21c–21h, 21t–26, 39d, 39e
Grzegorz Makarow – art. 21m–21s, 39c, 39l, 134, 138, 140
Agnieszka Skóra – art. 1, 4–6, 8, 21a, 21b, 21i–21l, 34
Karol Wach – art. 13–21, 26a–26c, 39f, 141, 142
Dawid Ziółkowski – art. 39i–39k

ISBN 978-83-8358-310-5 *ISBN PDF-a: 978-83-8358-564-2*

Wolters Kluwer Polska Sp. z o.o.
Dział Praw Autorskich
01-208 Warszawa, ul. Przyokopowa 33
tel. +48 728 313 462
e-mail: PL-ksiazki@wolterskluwer.com

księgarnia internetowa www.profinfo.pl

SPIS TREŚCI

WYKAZ SKRÓTÓW

Akty prawne

decyzja wykonawcza 2015/296	–	decyzja wykonawcza Komisji (UE) 2015/296 z 24.02.2015 r. ustanawiająca proceduralne warunki współpracy między państwami członkowskimi w zakresie identyfikacji elektronicznej na podstawie art. 12 ust. 7 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.Urz. UE L 53, s. 14)
decyzja wykonawcza 2015/1505	–	decyzja wykonawcza Komisji (UE) 2015/1505 z 8.09.2015 r. ustanawiająca specyfikacje techniczne i formaty dotyczące zaufanych list zgodnie z art. 22 ust. 5 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.Urz. UE L 235, s. 26)
decyzja wykonawcza 2015/1984	–	decyzja wykonawcza Komisji (UE) 2015/1984 z 3.11.2015 r. w sprawie określenia okoliczności, formatów i procedur notyfikacji zgodnie

		z art. 9 ust. 5 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym (notyfikowana jako dokument nr C(2015) 7369) (Dz.Urz. UE L 289, s. 18)
dyrektywa 1999/93/WE	–	dyrektywa Parlamentu Europejskiego i Rady 1999/93/WE z 13.12.1999 r. w sprawie wspólnotowych ram w zakresie podpisów elektronicznych (Dz.Urz. WE L 13, s. 12; uchylona)
k.c.	–	ustawa z 23.04.1964 r. – Kodeks cywilny (Dz.U. z 2023 r. poz. 1610 ze zm.)
k.k.	–	ustawa z 6.06.1997 r. – Kodeks karny (Dz.U. z 2024 r. poz. 17)
Konstytucja RP	–	Konstytucja Rzeczypospolitej Polskiej z 2.04.1997 r. (Dz.U. Nr 78, poz. 483 ze zm.)
k.p.a.	–	ustawa z 14.06.1960 r. – Kodeks postępowania administracyjnego (Dz.U. z 2023 r. poz. 775 ze zm.)
o.p.	–	ustawa z 29.08.1997 r. – Ordynacja podatkowa (Dz.U. z 2023 r. poz. 2383 ze zm.)
p.p.s.a.	–	ustawa z 30.08.2002 r. – Prawo o postępowaniu przed sądami administracyjnymi (Dz.U. z 2023 r. poz. 1634 ze zm.)
pr. bank.	–	ustawa z 29.08.1997 r. – Prawo bankowe (Dz.U. z 2023 r. poz. 2488)
pr. poczt.	–	ustawa z 23.11.2012 r. – Prawo pocztowe (Dz.U. z 2023 r. poz. 1640)
pr. przed.	–	ustawa z 6.03.2018 r. – Prawo przedsiębiorców (Dz.U. z 2023 r. poz. 221 ze zm.)
pr. upad.	–	ustawa z 28.02.2003 r. – Prawo upadłościowe (Dz.U. z 2022 r. poz. 1520 ze zm.)

p.s.w.n.	–	ustawa z 20.07.2018 r. – Prawo o szkolnictwie wyższym i nauce (Dz.U. z 2023 r. poz. 742 ze zm.)
p.u.s.a.	–	ustawa z 25.07.2002 r. – Prawo o ustroju sądów administracyjnych (Dz.U. z 2022 r. poz. 2492 ze zm.)
r.k.i.z.	–	rozporządzenie Ministra Cyfryzacji z 5.10.2016 r. w sprawie krajowej infrastruktury zaufania (Dz.U. poz. 1632)
r.KRI	–	rozporządzenie Rady Ministrów z 12.04.2012 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. z 2017 r. poz. 2247)
r.m.s.g.	–	rozporządzenie Ministra Finansów z 15.10.2018 r. w sprawie minimalnej sumy gwarancyjnej ubezpieczenia odpowiedzialności cywilnej podmiotu odpowiedzialnego za system identyfikacji elektronicznej (Dz.U. poz. 2009)
RODO	–	rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 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.Urz. UE L 119, s. 1, ze sprost.)
r.o.u.o.	–	rozporządzenie Ministra Rozwoju i Finansów z 19.12.2016 r. w sprawie obowiązkowego ubezpieczenia odpowiedzialności cywilnej kwalifikowanego dostawcy usług zaufania (Dz.U. z 2017 r. poz. 13)

rozporządzenie 765/2008	–	rozporządzenie Parlamentu Europejskiego i Rady (WE) nr 765/2008 z 9.07.2008 r. ustanawiające wymagania w zakresie akredytacji i nadzoru rynku odnoszące się do warunków wprowadzania produktów do obrotu i uchylające rozporządzenie (EWG) nr 339/93 (Dz.Urz. UE L 218, s. 30, ze zm.)
rozporządzenie 1316/2013	–	rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 1316/2013 z 11.12.2013 r. ustanawiające instrument „Łącząc Europę", zmieniające rozporządzenie (UE) nr 913/2010 oraz uchylające rozporządzenia (WE) nr 680/2007 i (WE) nr 67/2010 (Dz.Urz. UE L 348, s. 129)
rozporządzenie eIDAS	–	rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 910/2014 z 23.07.2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE (Dz.Urz. UE L 257, s. 73)
rozporządzenie wykonawcze 2015/1501	–	rozporządzenie wykonawcze Komisji (UE) 2015/1501 z 8.09.2015 r. w sprawie ram interoperacyjności na podstawie art. 12 ust. 8 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.Urz. UE L 235, s. 1, ze sprost.)
rozporządzenie wykonawcze 2015/1502	–	rozporządzenie wykonawcze Komisji (UE) 2015/1502 z 8.09.2015 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.Urz. UE L 235, s. 7, ze zm.)
r.w.k.o.	–	rozporządzenie Ministra Cyfryzacji z 6.09.2019 r. w sprawie wysokości kwot odpowiedzialności podmiotu odpowiedzialnego za system identyfikacji elektronicznej (Dz.U. poz. 1710)
TFUE	–	Traktat o funkcjonowaniu Unii Europejskiej (wersja skonsolidowana: Dz.Urz. UE C 202 z 2016 r., s. 47)
u.ABW	–	ustawa z 24.05.2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (Dz.U. z 2023 r. poz. 1136 ze zm.)
u.d.e.	–	ustawa z 18.11.2020 r. o doręczeniach elektronicznych (Dz.U. z 2023 r. poz. 285 ze zm.)
u.d.o.	–	ustawa z 6.08.2010 r. o dowodach osobistych (Dz.U. z 2022 r. poz. 671 ze zm.)
u.f.p.	–	ustawa z 27.08.2009 r. o finansach publicznych (Dz.U. z 2023 r. poz. 1270 ze zm.)
u.i.d.p.	–	ustawa z 17.02.2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz.U. z 2023 r. poz. 57 ze zm.)
u.k.a.r.	–	ustawa z 15.07.2011 r. o kontroli w administracji rządowej (Dz.U. z 2020 r. poz. 224)
u.KRS	–	ustawa z 20.08.1997 r. o Krajowym Rejestrze Sądowym (Dz.U. z 2023 r. poz. 685 ze zm.)
u.o.d.o.	–	ustawa z 10.05.2018 r. o ochronie danych osobowych (Dz.U. z 2019 r. poz. 1781)
u.o.i.n.	–	ustawa z 5.08.2010 r. o ochronie informacji niejawnych (Dz.U. z 2023 r. poz. 756 ze zm.)
u.p.e.	–	ustawa z 18.09.2001 r. o podpisie elektronicznym (Dz.U. z 2013 r. poz. 262 ze zm.; uchylona)

u.s.g.	–	ustawa z 8.03.1990 r. o samorządzie gminnym (Dz.U. z 2023 r. poz. 40 ze zm.)
u.u.z.i.	–	ustawa z 5.09.2016 r. o usługach zaufania oraz identyfikacji elektronicznej (Dz.U. z 2021 r. poz. 1797 ze zm.)
u.z.n.k.	–	ustawa z 16.04.1993 r. o zwalczaniu nieuczciwej konkurencji (Dz.U. z 2022 r. poz. 1233)
z.u.u.z.i.	–	ustawa z 5.07.2018 r. o zmianie ustawy o usługach zaufania oraz identyfikacji elektronicznej oraz niektórych innych ustaw (Dz.U. poz. 1544 ze zm.)

Dokumenty

PBI WK	–	Polityka Bezpieczeństwa Informacji dla Węzła Krajowego (wyciąg), wersja 3.0. z 14.01.2020 r., https://mc.bip.gov.pl/wezel-krajowy/wezel-krajowy-dokumentacja-dotyczaca-integracji-z-wezlem-krajowym.html (dostęp: 6.01.2024 r.)
Polityka Certyfikacji NCCert	–	Polityka Certyfikacji Narodowego Centrum Certyfikacji, wersja 3.6. z 1.12.2020 r. (OID: 1.3.6.1.4.1.31995.3.3.6), o której mowa w art. 10 ust. 2 u.u.z.i., dostępna pod adresem: https://www.nccert.pl/dokumenty.htm (dostęp: 6.01.2024 r.)
Standard	–	Standard publicznej usługi rejestrowanego doręczenia elektronicznego świadczonej przez operatora wyznaczonego i kwalifikowanych dostawców usług zaufania świadczących kwalifikowane usługi rejestrowanego doręczenia elektronicznego w zakresie współpracy z publiczną usługą rejestrowanego doręczenia elektronicznego oraz skrzynki doręczeń (wersja 1.1. z 3.06.2021 r.) udostępniony przez mini-

		stra właściwego do spraw informatyzacji na podstawie art. 26a u.u.z.i.
załącznik nr 1 do Standardu	–	ałącznik 1 do Standardu (wersja 1.1. z 3.06.2021 r.)

Czasopisma, zbiory orzecznictwa i wydawnictwa promulgacyjne

BGBl.	–	Bundesgesetzblatt
Dz.U.	–	Dziennik Ustaw
Dz.Urz. UE/WE	–	Dziennik Urzędowy Unii Europejskiej/Wspólnot Europejskich
iKAR	–	nternetowy Kwartalnik Antymonopolowy i Regulacyjny
Legalis	–	System Informacji Prawnej Legalis
LEX	–	System Informacji Prawnej LEX – wydawnictwa Wolters Kluwer Polska sp. z o.o.
MoP	–	Monitor Prawniczy
ONSA	–	Orzecznictwo Naczelnego Sądu Administracyjnego
OSNP	–	Orzecznictwo Sądu Najwyższego. Izba Pracy, Ubezpieczeń Społecznych i Spraw Publicznych
OSN-SD	–	Orzecznictwo Sądu Najwyższego – Sądu Dyscyplinarnego
OSP	–	Orzecznictwo Sądów Polskich
OTK-A	–	Orzecznictwo Trybunału Konstytucyjnego, Seria A
PiP	–	Państwo i Prawo
RPEiS	–	Ruch Prawniczy, Ekonomiczny i Socjologiczny

Inne

BIP	–	Biuletyn Informacji Publicznej

CBOSA	–	Centralna Baza Orzeczeń Sądów Administracyjnych
COI	–	Centralny Ośrodek Informatyki
ePUAP	–	elektroniczna Platforma Usług Administracji Publicznej
KIO	–	Krajowa Izba Odwoławcza
KIZ	–	krajowa infrastruktura zaufania
KRS	–	Krajowy Rejestr Sądowy
NBP	–	Narodowy Bank Polski
NCCert	–	narodowe centrum certyfikacji, o którym mowa w art. 2 pkt 3 u.u.z.i.
NSA	–	Naczelny Sąd Administracyjny
Rejestr	–	rejestr dostawców usług zaufania, o którym mowa w art. 2 pkt 1 i art. 3 u.u.z.i.
Rejestr Systemów	–	rejestr systemów identyfikacji elektronicznej przyłączonych do węzła krajowego, o którym mowa w art. 21n u.u.z.i.
SA	–	Sąd Apelacyjny
SHA-1	–	Secure Hash Algoritm 1
SN	–	Sąd Najwyższy
Szef ABW	–	Szef Agencji Bezpieczeństwa Wewnętrznego
TS	–	Trybunał Sprawiedliwości
UE	–	Unia Europejska
węzeł krajowy	–	węzeł krajowy identyfikacji elektronicznej, o którym mowa w art. 21a ust. 1 pkt 1 i ust. 2 u.u.z.i.
węzeł transgraniczny	–	węzeł wykorzystywany w procesie transgranicznego uwierzytelniania osób, o którym mowa w art. 21a ust. 1 pkt 3 u.u.z.i.
WSA	–	Wojewódzki Sąd Administracyjny

WSTĘP

Współczesne rozwiązania technologiczne są coraz powszechniej wykorzystywane w codziennym funkcjonowaniu przez jednostki, a także inne podmioty, w tym organy władzy publicznej. Warto wskazać w szczególności na podpis elektroniczny, pieczęć elektroniczną, elektroniczny znacznik czasu, rejestrowane doręczenia elektroniczne czy identyfikację elektroniczną. Wykorzystanie tych narzędzi w obiegu prawnym jest teraz przedmiotem szczegółowych uregulowań na szczeblu Unii Europejskiej oraz w prawodawstwie krajowym.

Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 910/2014 z 23.07.2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE (Dz.Urz. UE L 257, s. 73; rozporządzenie eIDAS) weszło w życie 17.09.2014 r., a stosuje się je od 1.07.2016 r. Wprowadziło ono nowy porządek prawny w obszarze identyfikacji elektronicznej oraz usług zaufania, obejmujących m.in.: podpis elektroniczny, pieczęć elektroniczną, elektroniczny znacznik czasu i usługę rejestrowanego doręczenia elektronicznego. Akt ten (wraz z systemem aktów wykonawczych) obowiązuje na terenie Unii Europejskiej w sposób bezpośredni (tzw. bezpośrednia skuteczność), nie wymagał więc implementacji do prawa krajowego poszczególnych państw członkowskich. W kilku regulowanych przez niego obszarach pozostawiono jednak ustawodawcy krajowemu swobodę normatywną, m.in. w zakresie: określenia porządku instytucjonalnego przewidzianego rozporzą-

dzeniem eIDAS, wymogu ustanowienia nadzoru nad usługami zaufania, ustalenia zasady odpowiedzialności cywilnoprawnej dostawców usług zaufania. Jednocześnie uregulowania wprowadzone w tym rozporządzeniu unijnym spowodowały konieczność dostosowania prawa krajowego do nowych rozwiązań normatywnych i nowej terminologii. Poszczególni ustawodawcy krajowi zostali zatem zobowiązani do ustanowienia norm prawnych regulujących zagadnienia wskazane przez rozporządzenie eIDAS (które pozostawiono w kompetencji państw członkowskich) oraz do dokonania koniecznych zmian w aktach rangi ustawowej (i równoważnych) dla prawidłowego realizowania przepisów tego rozporządzenia unijnego. Dlatego w Polsce uchwalona została ustawa z 5.09.2016 r. o usługach zaufania oraz identyfikacji elektronicznej (Dz.U. z 2021 r. poz. 1797 ze zm.), która obowiązuje od 7.10.2016 r.

Polska ustawa o usługach zaufania oraz identyfikacji elektronicznej reguluje dwa istotne obszary: identyfikację elektroniczną oraz usługi zaufania. W szczególności określa: krajową infrastrukturę zaufania, działalność dostawców usług zaufania (w tym zawieszanie certyfikatów podpisów elektronicznych i pieczęci elektronicznych), tryb notyfikacji krajowego systemu identyfikacji elektronicznej, nadzór nad dostawcami usług zaufania, krajowy schemat identyfikacji elektronicznej, nadzór nad krajowym schematem identyfikacji elektronicznej, a także zawiera przepisy karne. Ustawodawca w uzasadnieniu projektu omawianej ustawy podkreślił, że jej głównym celem jest stworzenie warunków do realizacji rozporządzenia eIDAS. Chodzi o dostosowanie krajowego porządku prawnego do rozwiązań zawartych w tym akcie prawa unijnego oraz wyeliminowanie wszelkich przepisów z nim niezgodnych. Ponadto ma ona regulować te obszary prawa, które są niezbędne do umożliwienia stosowania rozporządzenia eIDAS na gruncie prawa polskiego, oraz dostosować krajowy porządek prawny w zakresie nowych instytucji prawnych i nowej terminologii[1].

[1] Rządowy projekt ustawy o usługach zaufania oraz identyfikacji elektronicznej, druk sejmowy nr 713, VII kadencja Sejmu RP, s. 79.

Prezentowany komentarz do ustawy o usługach zaufania oraz identyfikacji elektronicznej, przygotowany przez Autorów, pod naszą redakcją, stanowi pierwszą kompleksową analizę przepisów tego aktu prawnego wraz z opisem ich funkcjonowania. Ponadto w opracowaniu zawarte zostały praktyczne wyjaśnienia dotyczące ich stosowania. Jednocześnie – ze względu na chęć przybliżenia Czytelnikom tej problematyki – Autorzy nawiązują również do polskich przepisów prawa administracyjnego, cywilnego oraz karnego. Poglądy i wnioski zaprezentowane przez Autorów są wynikiem ich wieloletniego doświadczenia naukowego oraz zawodowego związanego ze stosowaniem prawa w ramach pracy w administracji publicznej lub w sektorze prywatnym. Komentując przepisy, Autorzy wyrażają własne stanowisko.

Komentarz jest przeznaczony dla sędziów, adwokatów, radców prawnych, doradców podatkowych, rzeczników patentowych oraz pracowników organów władzy publicznej, a także pracowników naukowych oraz studentów. Mamy nadzieję, że zawarte w nim rozważania prawne okażą się pomocne w rozwiązywaniu konkretnych zagadnień.

Stan prawny: 6.01.2024 r.

Gdańsk–Warszawa, styczeń 2024 r.

dr hab. Agnieszka Skóra, prof. UWM
dr Błażej Kwiatek

USTAWA

z dnia 5 września 2016 r.

o usługach zaufania oraz identyfikacji elektronicznej[1]

(tekst jedn. Dz.U. z 2021 r. poz. 1797; zm.: Dz.U. z 2023 r. poz. 1234)

[1] Niniejsza ustawa służy stosowaniu rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 z 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylającego dyrektywę 1999/93/WE (Dz.Urz. UE L 257 z 28.08.2014, s. 73).

ROZDZIAŁ 1

Przepisy ogólne

Art. 1. [Zakres stosowania ustawy; pojęcia usługi zaufania i identyfikacji elektronicznej]

1. Ustawa określa:

1) **krajową infrastrukturę zaufania;**
2) **działalność dostawców usług zaufania, w tym zawieszanie certyfikatów podpisów elektronicznych i pieczęci elektronicznych;**
3) **tryb notyfikacji krajowego systemu identyfikacji elektronicznej;**
4) **nadzór nad dostawcami usług zaufania;**
5) **krajowy schemat identyfikacji elektronicznej;**
6) **nadzór nad krajowym schematem identyfikacji elektronicznej;**
7) **zasady określania i wykorzystywania standardu usługi rejestrowanego doręczenia elektronicznego.**

2. Przepisów ustawy nie stosuje się do identyfikacji elektronicznej lub świadczenia usług zaufania wykorzystywanych wyłącznie w zamkniętych systemach wynikających z przepisów prawa, porozumień lub umów zawartych przez określoną grupę uczestników.

1. Ustawa o usługach zaufania oraz identyfikacji elektronicznej została uchwalona przez polskiego ustawodawcę w związku z wejściem w życie rozporządzenia eIDAS, które wprowadziło we wszystkich krajach Unii Europejskiej nowy porządek prawny w obszarze usług zaufania oraz identyfikacji elektronicznej. Akt ten obowiązuje na terenie UE w sposób bezpośredni. Moc prawna rozporządzenia eIDAS nie jest więc uzależniona od obligatoryjnego aktu implementacji jego przepisów do prawa krajowego[2], wyklucza także możliwość jego zmiany bądź modyfikacji przez państwa członkowskie. Państwa członkowskie mają jednak prawo „doprecyzowania" tych obszarów regulacji, które prawodawca unijny pozostawił niedookreślone lub wprost odesłał do prawa krajowego – pod warunkiem, że sposób tego doprecyzowania nie będzie stał na przeszkodzie osiągnięciu celów rozporządzenia[3].

Podstawowa idea rozporządzenia eIDAS wyraża się przede wszystkim – zgodnie z jego motywem 2 – w zwiększeniu zaufania do transakcji elektronicznych na rynku wewnętrznym poprzez zapewnienie wspólnej podstawy bezpiecznych interakcji elektronicznych między obywatelami, przedsiębiorstwami i organami publicznymi, co ma podnieść efektywność publicznych i prywatnych usług online, e-biznesu i e-handlu w UE. Pojęcie transakcji należy przy tym rozumieć szerzej niż transakcje handlowe, a mianowicie w sposób zbliżony do słowa „proces" w jego potocznym rozumieniu[4] (tj. jako „przebieg następujących po sobie i powiązanych przyczynowo określonych zmian")[5]. Celem ustawodawcy unijnego była przede wszystkim unifikacja rozwiązań prawnych we wszystkich

---

2 Por. D. Drypa, *Opinia do ustawy o usługach zaufania oraz identyfikacji elektronicznej*, druk sejmowy nr 268, VIII kadencja Sejmu RP, s. 1 i n.

3 A. Romaszewski, W. Trąbka, M. Kielar, K. Gajda, *Wprowadzenie usług zaufania zgodnych z rozporządzeniem UE eIDAS w aspekcie systemów informacyjnych opieki zdrowotnej*, cz. 1, „Zeszyt Naukowy Wyższej Szkoły Zarządzania i Bankowości w Krakowie" 2016/42, s. 25.

4 Ł. Goździaszek, *Identyfikacja elektroniczna i usługi zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym Unii Europejskiej. Komentarz*, Legalis 2019, komentarz do art. 1 rozporządzenia eIDAS.

5 Internetowy *Słownik języka polskiego PWN*, hasło „proces", https://sjp.pwn.pl/szukaj/proces.html (dostęp: 6.01.2024 r.).

państwach UE w zakresie wskazanych w tym rozporządzeniu usług zaufania i identyfikacji elektronicznej oraz podniesienie poziomu ich bezpieczeństwa, a także zapewnienie w ten sposób integracji i transgranicznego charakteru[6]. Rozporządzenie eIDAS uporządkowało katalog usług zaufania. W Polsce akt ten doprowadził do poszerzenia dostępnych usług zaufania, gdyż przed jego wejściem w życie regulowane w sposób pełny były jedynie podpis elektroniczny oraz znakowanie czasem. Natomiast w niektórych innych państwach (np. w Czechach) przed wejściem w życie rozporządzenia eIDAS funkcjonujący w obrocie krajowym katalog usług zaufania był szerszy[7].

Wspomniany akt unijny wprowadził także we wszystkich państwach członkowskich UE jednolitą terminologię stosowaną w zakresie usług zaufania i identyfikacji elektronicznej. Nałożył również na te państwa obowiązek ustanowienia nadzoru nad dostawcami usług zaufania oraz określił tryb notyfikowania systemów identyfikacji elektronicznej. W rozporządzeniu eIDAS przewidziano bowiem tzw. zasadę wzajemnego uznawania środków identyfikacji elektronicznej (art. 6 rozporządzenia eIDAS) oraz procedurę notyfikowania tych systemów w Komisji UE (art. 7–9 rozporządzenia eIDAS). Warto jednak zwrócić uwagę, że na gruncie prawa polskiego nie wszystkie systemy identyfikacji elektronicznej powinny być obowiązkowo notyfikowane – ustawa o usługach zaufania oraz identyfikacji elektronicznej nie przewiduje takiej powinności.

2. Rozporządzenie eIDAS weszło w życie 17.09.2014 r. Przepis art. 52 ust. 2 tego aktu unijnego określił, że stosuje się je od 1.07.2016 r., z wyjątkiem przepisów *expressis verbis* w nim wymienionych. Zarazem 1.07.2016 r. utraciła moc dyrektywa Parlamentu Europejskiego i Rady

[6] Na ten aspekt zwracają uwagę m.in.: P.P. Polański, *Towards the single digital market for e-identification and trust services*, „Computer Law & Security Review" 2015/31, s. 774–775; J. Dumortier, N. Vandezande, *Trust in the proposed EU regulation on trust services?*, „Computer Law & Security Review" 2012/28, s. 568.

[7] Szerzej na temat celów rozporządzenia eIDAS w relacji do prawa państw członkowskich zob. P.P. Polański, *Towards...*, s. 773.

1999/93/WE z 13.12.1999 r. w sprawie wspólnotowych ram w zakresie podpisów elektronicznych (Dz.Urz. WE L 13, s. 12), od tego dnia obowiązuje większość przepisów dotyczących usług zaufania uregulowanych w rozporządzeniu eIDAS. Polska ustawa z 18.09.2001 r. o podpisie elektronicznym (Dz.U. z 2013 r. poz. 262 ze zm.) przestała obowiązywać 6.10.2016 r. Straciły także moc przepisy dotyczące transakcji elektronicznych, które obowiązywały przed 1.07.2016 r. na terenie Polski i nie były zgodne z rozwiązaniami prawnymi rozporządzenia eIDAS. Ustawa o usługach zaufania oraz identyfikacji elektronicznej weszła w życie 7.10.2016 r., z wyjątkami w niej wskazanymi (zob. szerzej komentarz do art. 142 u.u.z.i.). Od 29.09.2018 r. istnieje obowiązek wzajemnego uznawania przez państwa członkowskie notyfikowanych systemów identyfikacji elektronicznej.

3. Inne państwa członkowskie Unii Europejskiej także uchwaliły akty normatywne dostosowujące ich porządek prawny do rozwiązań przewidzianych w rozporządzeniu eIDAS, jak np.: Republika Czeska – *Zákon o službách vytvářejících důvěru pro elektronické transakce* (Zákon č. 297/2016 Sb.)[8], Republika Słowacka – *Zákon z 20. septembra 2016 o dôveryhodných službách pre elektronické transakcie na vnútornom trhu a o zmene a doplnení niektorých zákonov (zákon o dôveryhodných službách* – 272/2016[9], Republika Litwy – *Elektroninės atpažinties ir elektroninių operacijų patikimumo užtikrinimo paslaugų Įstatymas* (Nr XIII-1120)[10], Republika Estonii – *E-identimise ja e-tehingute usaldusteenuste seadus* (RT I, 25.10.2016, 1)[11], Republika Austrii – *Bundesgesetz über elektronische Signaturen und Vertrauensdienste für elektronische Transaktionen (Signatur- und Vertrauensdienstegesetz – SVG*, BGBl. I Nr 50/2016)[12], Bułgaria – *Закон за електронния документ*

[8] Zob.: https://www.zakonyprolidi.cz/cs/2016-297/zneni-20230401 (dostęp: 6.01.2024 r.).
[9] Zob.: https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2016/272/ (dostęp: 6.01.2024 r.).
[10] Zob.: https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/994308704dfa11e88525a4bc7611b788 (dostęp: 6.01.2024 r.).
[11] Zob.: https://www.riigiteataja.ee/akt/125102016001 (dostęp: 6.01.2024 r.).
[12] Zob. https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20009585 (dostęp: 6.01.2024 r.).

и електронните удостоверителни услуги (загл. Изм. - дв, бр. 85 от 2017 г.)[13], Królestwo Danii – *Lov om supplerende bestemmelser til forordning om elektronisk identifikation og tillidstjenester til brug for elektroniske transaktioner på det indre marked*, nr 617 af 8 juni 2016[14], Republika Federalna Niemiec – *Gesetz zur Durchführung der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG (eIDAS-Durchführungsgesetz)*[15], Królestwo Szwecji – *Lag (2016:561) med kompletterande bestämmelser till EU:s förordning om elektronisk identifiering*[16].

4. Wprowadzenie nowych rozwiązań w zakresie usług zaufania i identyfikacji elektronicznej przez rozporządzenie eIDAS zrodziło konieczność dostosowania do nich prawa polskiego. Zamiarem rodzimego ustawodawcy, wyrażonym w uzasadnieniu projektu ustawy o usługach zaufania oraz identyfikacji elektronicznej, było uchwalenie przepisów w odniesieniu do kwestii wskazanych przez rozporządzenie eIDAS jako pozostających w kompetencji państw członkowskich oraz dokonanie zmian w aktach rangi ustawowej koniecznych do prawidłowej realizacji rozporządzenia eIDAS[17].

Przepis art. 1 u.u.z.i. określa przedmiot regulacji ustawy o zasługach zaufania oraz identyfikacji elektronicznej. Większość przepisów komentowanej ustawy poświęcona jest regulacji dwóch istotnych obszarów: systemów identyfikacji elektronicznej oraz usług zaufania. W zakresie usług zaufania akt ten określa w szczególności krajową infrastrukturę

[13] Zob.: https://lex.bg/laws/ldoc/2135180800 (dostęp: 6.01.2024 r.).

[14] Zob.: https://www.ft.dk/samling/20151/lovforslag/l119/index.htm (dostęp: 6.01.2024 r.).

[15] BGBl. I S. 2745, https://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&start=//*%5b@attr_id=%27bgbl117s2745.pdf%27%5d#__bgbl__%2F%2F*%5B%40attr_id%3D%27bgbl117s2745.pdf%27%5D__1703070468130 (dostęp: 6.01.2024 r.).

[16] Zob.: https://www.riksdagen.se/sv/dokument-och-lagar/dokument/svensk-forfattningssamling/lag-2016561-med-kompletterande-bestammelser_sfs-2016-561/ (dostęp: 6.01.2024 r.).

[17] Zob. D. Drypa, *Opinia...*, s. 1.

zaufania, działalność dostawców usług zaufania (w tym zawieszanie certyfikatów podpisów elektronicznych i pieczęci elektronicznych) oraz nadzór nad dostawcami usług zaufania. Natomiast w obszarze identyfikacji elektronicznej omawiana ustawa normuje przede wszystkim krajowy schemat identyfikacji elektronicznej, tryb notyfikacji krajowego systemu identyfikacji elektronicznej (art. 24 u.u.z.i.) oraz nadzór (w tym środki nadzorcze i organ nadzoru) nad krajowym schematem identyfikacji elektronicznej. Reguluje także odpowiedzialność karną (rozdział 6, art. 40–45 u.u.z.i.) oraz karno-administracyjną (rozdział 7, art. 46–49 u.u.z.i.). Określenie sankcji za naruszenie regulacji wprowadzonej przez rozporządzenie eIDAS pozostawione zostało bowiem poszczególnym państwom członkowskim do własnego unormowania.

5. Na podstawie przepisów ustawy o usługach zaufania oraz identyfikacji elektronicznej wydane zostały następujące akty wykonawcze: rozporządzenie Ministra Cyfryzacji z 5.10.2016 r. w sprawie krajowej infrastruktury zaufania (Dz.U. poz. 1632); rozporządzenie Ministra Cyfryzacji z 6.09.2019 r. w sprawie wysokości kwot odpowiedzialności podmiotu odpowiedzialnego za system identyfikacji elektronicznej (Dz.U. poz. 1710); rozporządzenie Rady Ministrów z 6.11.2018 r. w sprawie zakresu danych i dokumentów niezbędnych do przeprowadzenia postępowania w celu dokonania oceny korporacyjnej podmiotu odpowiedzialnego za system identyfikacji elektronicznej lub podmiotu wydającego środki identyfikacji elektronicznej w tym systemie (Dz.U. poz. 2207); rozporządzenie Ministra Finansów z 15.10.2018 r. w sprawie minimalnej sumy gwarancyjnej ubezpieczenia odpowiedzialności cywilnej podmiotu odpowiedzialnego za system identyfikacji elektronicznej (Dz.U. poz. 2009); rozporządzenie Ministra Rozwoju i Finansów z 19.12.2016 r. w sprawie obowiązkowego ubezpieczenia odpowiedzialności cywilnej kwalifikowanego dostawcy usług zaufania (Dz.U. z 2017 r. poz. 13).

6. Nieobowiązujące już dyrektywa 1999/93/WE i polska ustawa o podpisie elektronicznym nie posługiwały się terminem „usługa zaufania" (ang. *trust service*). Jest to nowy termin, po raz pierwszym użyty w rozporzą-

dzeniu eIDAS, a następnie wprowadzony przez rodzimego ustawodawcę do komentowanej ustawy. Celem tej usługi jest stworzenie ram prawnych dla zapewnienia zaufania i bezpieczeństwa transakcji elektronicznych dokonywanych przez obywateli oraz inne podmioty w państwach UE. Jak trafnie uważa I. Jóźwiak, wspólną cechą usług zaufania jest ich ukierunkowanie na wyeliminowanie anonimowości podmiotów dokonujących czynności drogą elektroniczną i „jednoczesne uwiarygodnienie ich działań poprzez m.in. uwierzytelnienie tożsamości" podmiotu dokonującego czynności, „zapewnienie integralności (niezmienności) treści składanych oświadczeń woli, potwierdzenie czasu dokonania czynności"[18]. W motywie 1 rozporządzenia eIDAS wskazano, że brak zaufania „sprawia, że konsumenci, organy publiczne i przedsiębiorstwa wahają się, czy przeprowadzać transakcje elektroniczne i wdrażać nowe usługi".

„Usługa zaufania" zdefiniowana została przez prawodawcę unijnego w art. 3 pkt 16 rozporządzenia eIDAS jako usługa elektroniczna (zasadniczo świadczona za wynagrodzeniem, czyli odpłatna), której celem jest tworzenie, weryfikacja, walidacja i konserwacja podpisów elektronicznych, pieczęci elektronicznych, certyfikatów uwierzytelnienia witryn internetowych. W świetle przywołanej definicji usługa zaufania charakteryzuje się kilkoma istotnymi cechami.

Mimo że pojęcie zaufania używane jest w wielu przepisach oraz w różnych kontekstach w rozporządzeniu eIDAS i w ustawie o usługach zaufania oraz identyfikacji elektronicznej, jego znaczenie jest niejasne[19]. J. Dumortier i N. Vandezande przyjmują, że rozporządzenie eIDAS pojęcie zaufania ujmuje w sposób kompleksowy, łącząc w nim elementy wywodzące się z nauk psychologicznych, socjologicznych oraz ekonomicznych[20]. I tak, ich zadaniem zaufanie można postrzegać jako zwią-

[18] I. Jóźwiak, *Odpowiedzialność dostawców usług zaufania – wybrane aspekty*, „Człowiek w cyberprzestrzeni" 2018/3, s. 37.

[19] Na gruncie rozporządzenia eIDAS zwracają na to uwagę J. Dumortier i N. Vandezande, *Trust...*, s. 573.

[20] J. Dumortier, N. Vandezande, *Trust...*, s. 574.

zane z relacjami międzyludzkimi, wiążącymi się z pewnym poziomem ryzyka[21]. Autorzy ci przyjmują, że zaufania oczekuje się od użytkownika (podmiotu) transakcji. Podmiot ten z kolei oczekuje określonego poziomu wiarygodności i bezpieczeństwa od dostawcy usługi zaufania. W tym świetle usługi zaufania mogą być postrzegane jako „usługi godne zaufania" (ang. *trustworthy services*).

Usługa zaufania, po pierwsze, obejmuje jedno z trzech możliwych działań. Pierwsze z nich może dotyczyć tworzenia, weryfikacji lub walidacji podpisów elektronicznych, a także znaczników czasu lub pieczęci, usług rejestrowanych doręczeń elektronicznych oraz certyfikatów wymaganych przy tych usługach. Drugie działanie obejmuje tworzenie, weryfikację oraz walidację certyfikatów, które służą do uwierzytelniania stron internetowych. Trzecim działaniem jest zachowanie (konserwacja) podpisów elektronicznych, pieczęci lub powiązanych z nimi certyfikatów[22]. Na marginesie należy dodać, że w art. 1 pkt 3 lit. d projektu rozporządzenia Parlamentu Europejskiego i Rady zmieniającego rozporządzenie (UE) nr 910/2014 w odniesieniu do ustanowienia europejskich ram tożsamości cyfrowej[23] (tzw. eIDAS 2) przewidziano nowe usługi zaufania, tj.: tworzenie, weryfikację i walidację elektronicznego poświadczenia atrybutów oraz certyfikatów powiązanych z tymi usługami, archiwizację elektroniczną dokumentów elektronicznych, zarządzanie urządzeniami do składania podpisów i pieczęci elektronicznych na odległość oraz zapisywanie danych elektronicznych w rejestrze elektronicznym.

Po drugie, usługi zaufania zostały zakwalifikowane jako usługi elektroniczne. Jako takie są ściśle związane z usługami społeczeństwa informacyjnego, realizowanymi na odległość, drogą elektroniczną i na indywi-

[21] J. Dumortier, N. Vandezande, *Trust*..., s. 574.

[22] A. Monarcha-Matlak, *Usługi zaufania i identyfikacja elektroniczna*, „Acta Iuris Stetinensis" 2018/3, s. 144.

[23] Bruksela, dnia 3.6.2021 r., COM(2021) 281 final. Projekt dostępny pod adresem: https://eur-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=CELEX:52021PC0281 (dostęp: 6.01.2024 r.).

dualne żądanie użytkownika[24]. Trzeba jednak pamiętać o częściowo odmiennym zakresie pojęć usługi świadczonej na odległość i usługi elektronicznej. Usługi świadczone na odległość to usługi dokonywane bez jednoczesnej fizycznej obecności stron za pomocą tzw. środków komunikacji na odległość[25]. Usługi zaufania realizowane są natomiast wyłącznie jako usługi elektroniczne (tj. w środowisku elektronicznym), zwykle drogą elektroniczną, nie zaś za pomocą innych środków komunikacji na odległość (jakimi są np. media drukowane: formularze, listy seryjne, reklamy prasowe z wydrukowanym wzorem zamówienia; środki komunikacji telefonicznej, tj. telefon, telefaks, a także środki komunikacji radiowej i telewizyjnej)[26].

Po trzecie, usługi zaufania zostały określone jako zazwyczaj odpłatne, tj. świadczone za wynagrodzeniem[27]. Definicja usługi zaufania jest zatem spójna z zawartą w art. 57 TFUE definicją usługi, która wymaga bezpośredniego (od usługobiorcy)[28] lub pośredniego (np. od reklamodawcy) wynagrodzenia za usługę[29]. Charakter odpłatny świadczenia usług nie zawsze bowiem oznacza, że za usługę musi płacić bezpośredni usługobiorca, czyli konsument[30].

---

24 P.P. Polański, *Towards...*, s. 777.

25 Por. art. 2 pkt 7 oraz motyw 20 dyrektywy Parlamentu Europejskiego i Rady 2011/83/UE z 25.10.2011 r. w sprawie praw konsumentów, zmieniającej dyrektywę Rady 93/13/EWG i dyrektywę 1999/44/WE Parlamentu Europejskiego i Rady oraz uchylającej dyrektywę Rady 85/577/EWG i dyrektywę 97/7/WE Parlamentu Europejskiego i Rady, Dz.Urz. UE L 304, s. 64.

26 Na temat środków komunikowania się na odległość zob. m.in. M. Maciejewska-Szałas, *Wybrane zagadnienia problematyki zawarcia umowy na odległość w świetle ustawy o prawach konsumenta*, „Gdańskie Studia Prawnicze" 2017/1, s. 293.

27 Na cechę odpłatności wskazuje m.in. P.P. Polański, *Towards...*, s. 777.

28 Zob. na temat cechy odpłatności usługi m.in.: wyrok TS z 27.09.1988 r. w sprawie C-263/86, Humbel, ECLI:EU:C:1988:451 i wyrok TS z 3.03.1994 r. w sprawie C-16/93, Tolsma, ECLI:EU:C:1994:80.

29 Zob. na temat pośredniej odpłatności za usługę m.in. wyrok TS z 26.04.1988 r. w sprawie C-352/85, Bond van Adverteerders, ECLI:EU:C:1988:196.

30 E. Skrzydło-Tefelska, komentarz do art. 57 TFUE [w:] *Traktat o funkcjonowaniu Unii Europejskiej. Komentarz*, t. 1 (art. 1–89), red. D. Miąsik, N. Półtorak, A. Wróbel, Warszawa 2012.

7. Jak już wspomniano, celem rozporządzenia eIDAS było wprowadzenie we wszystkich państwach Unii Europejskiej jednolitego nazewnictwa i charakteru prawnego usług zaufania. Katalog kwalifikowanych usług zaufania wymienionych w art. 3 pkt 16 rozporządzenia eIDAS ma charakter zamknięty[31] w tym sensie, że nie stanowi on jedynie ich przykładowego wyliczenia[32]. Wskazane w nim usługi można określić jako „nazwane" kwalifikowane usługi zaufania. Są to:

1) tworzenie, weryfikacja i walidacja podpisów elektronicznych, pieczęci elektronicznych lub elektronicznych znaczników czasu, usług rejestrowanego doręczenia elektronicznego oraz certyfikatów powiązanych z tymi usługami;
2) tworzenie, weryfikacja i walidacja certyfikatów uwierzytelniania witryn internetowych;
3) konserwacja elektronicznych podpisów, pieczęci lub certyfikatów powiązanych z tymi usługami.

W świetle motywu 25 rozporządzenia eIDAS państwom członkowskim pozostawiono swobodę określania w przepisach prawa krajowego także innych rodzajów usług zaufania, zarówno „zwykłych", jak i kwalifikowanych[33]. Motyw 26 rozporządzenia eIDAS stanowi bowiem, że z uwagi „na tempo zmian technologicznych należy przyjąć podejście otwarte na innowacje". Podzielić więc należy pogląd między innymi Ł. Goździaszka, że przepisy tego rozporządzenia nie stoją na przeszkodzie uregulowaniu na szczeblu krajowym innych kwalifikowanych usług zaufania, o ile w pełni respektowane będą regulacje rozporządzenia eIDAS, w szczególności jego art. 20–24. Jednak usługi krajowe nie mogą „stanowić takiej modyfikacji wymienionych w rozporządzeniu eIDAS kwalifikowanych usług zaufania"[34], która „wypacza" ich sens i stanowi tym samym „obej-

[31] M. Marucha-Jaworska, *Rozporządzenie eIDAS. Zagadnienia prawne i techniczne*, Warszawa 2017, s. 49; A. Anusz, *Ochrona konsumentów w świetle rozporządzenia eIDAS*, iKAR 2020/2, s. 102.

[32] Ł. Goździaszek, *Identyfikacja...*, komentarz do art. 3 rozporządzenia eIDAS.

[33] Tak m.in.: Ł. Goździaszek, *Identyfikacja...*, komentarz do art. 3 rozporządzenia eIDAS; M. Marucha-Jaworska, *Rozporządzenie...*, s. 49.

[34] Ł. Goździaszek, *Identyfikacja...*, komentarz do art. 3 rozporządzenia eIDAS.

ście wymogów przewidzianych dla konkretnych rodzajów kwalifikowanych usług zaufania"[35]. Usługi zaufania – regulowane na szczeblu krajowym – niewymienione *expressis verbis* w rozporządzeniu eIDAS można określić jako „nienazwane" usługi zaufania.

Na marginesie warto dodać, że niektóre z bezpośrednio wymienionych w rozporządzeniu eIDAS kwalifikowanych usług zaufania są regulowane w sposób ogólny (np. kwalifikowana usługa rejestrowanego doręczenia elektronicznego). Prawodawca unijny nie narzucił także usługom zaufania określonych rozwiązań technologicznych (tzw. zasada neutralności technologicznej). Motyw 27 rozporządzenia eIDAS stanowi, że: „Określone w nim skutki prawne powinny być osiągalne za pomocą dowolnego środka technicznego, o ile spełnione zostaną wymogi niniejszego rozporządzenia".

W świetle rozporządzenia eIDAS usługi zaufania spełniające określone w nim wymagania powinny podlegać swobodnemu obrotowi na rynku wewnętrznym UE. Zgodnie z treścią art. 4 ust. 1 i 2 tego aktu unijnego: „1. Nie ogranicza się świadczenia usług zaufania na terytorium państwa członkowskiego przez dostawcę usług zaufania mającego siedzibę w innym państwie członkowskim z powodów związanych z dziedzinami objętymi niniejszym rozporządzeniem. 2. Produkty i usługi zaufania spełniające wymogi niniejszego rozporządzenia dopuszcza się do swobodnego obrotu na rynku wewnętrznym".

8. W celu nadania usłudze zaufania statusu kwalifikowanego niezbędne jest spełnienie przez usługę wymagań określonych w rozporządzeniu eIDAS (art. 3 pkt 17 rozporządzenia eIDAS).

9. Przepis art. 1 ust. 2 u.u.z.i. *expressis verbis* stanowi, że komentowanej ustawy nie stosuje się do identyfikacji elektronicznej lub świadczenia usług zaufania wykorzystywanych wyłącznie w zamkniętych systemach wynikających z przepisów prawa, porozumień lub umów zawartych

[35] Ł. Goździaszek, *Identyfikacja...*, komentarz do art. 3 rozporządzenia eIDAS.

przez określoną grupę uczestników. Treść tego przepisu koresponduje z art. 2 ust. 2 oraz motywem 21 zdanie 2 rozporządzenia eIDAS, w świetle których ten akt unijny nie obejmuje zakresem „świadczenia usług zaufania [rozporządzenie eIDAS nie wspomina jednak o identyfikacji elektronicznej – przyp. A.S.] wykorzystywanych wyłącznie w obrębie zamkniętych systemów wynikających z prawa krajowego lub z porozumień zawartych przez określoną grupę uczestników" (art. 2 ust. 2 rozporządzenia eIDAS) i niemających skutków dla stron trzecich. Zgodnie z treścią motywu 21 rozporządzenia eIDAS wymogom tego rozporządzenia „nie powinny na przykład podlegać systemy utworzone w przedsiębiorstwach lub administracjach publicznych w celu zarządzania procedurami wewnętrznymi przy użyciu usług zaufania. Wymogi określone w rozporządzeniu powinny spełniać jedynie usługi zaufania świadczone na rzecz społeczeństwa, mające skutki dla stron trzecich". Takimi systemami zamkniętymi są na przykład: system pracowników administracji szpitala służący do obsługi wewnętrznych dokumentów tworzonych i akceptowanych przez pracowników różnych komórek organizacyjnych[36], bankowość elektroniczna czy schematy płatności w handlu elektronicznym oferowane wyłącznie klientom banków lub sklepów internetowych[37].

Przepisy art. 1 ust. 2 u.u.z.i. oraz art. 2 ust. 2 i motyw 21 zdanie 2 rozporządzenia eIDAS pozwalają na wyróżnienie tzw. otwartych oraz zamkniętych usług zaufania. „Otwarte" usługi zaufania realizowane są na rzecz społeczeństwa i mogą (jakkolwiek nie muszą) wywierać skutki dla stron trzecich. „Otwarte" usługi zaufania podlegają wymaganiom stawianym przez rozporządzenie eIDAS, ustawę o usługach zaufania oraz identyfikacji elektronicznej, a także akty wykonawcze do nich. „Zamknięte" usługi zaufania są świadczone na rzecz określonej, dobrze zdefiniowanej grupy użytkowników i nie wywierają skutków wobec stron trzecich. Podstawą ich świadczenia są przepisy prawa, porozumienia lub umowy zawarte przez określoną grupę uczestników. Usługi te są

[36] A. Romaszewski, W. Trąbka, M. Kielar, K. Gajda, *Wprowadzenie...*, s. 28.
[37] P.P. Polański, *Towards...*, s. 774.

świadczone w ramach zamkniętego systemu teleinformatycznego[38]. Jak wspomniano wyżej, „zamknięte" usługi zaufania są *expressis verbis* wyłączone z zakresu regulacji przez art. 2 ust. 2 rozporządzenia eIDAS i nie podlegają jego przepisom[39].

Podział na usługi „otwarte" i „zamknięte" ma istotne znaczenie dla systemów teleinformatycznych funkcjonujących między innymi w ochronie zdrowia i w tym obszarze dotyczy zarówno systemów planowanych na szczeblu ogólnokrajowym, jak i systemów już funkcjonujących w szpitalach i poradniach w lecznictwie otwartym[40].

10. Komentowana ustawa normuje także zagadnienia związane z identyfikacją elektroniczną, tj. krajowy schemat identyfikacji elektronicznej, nadzór nad krajowym schematem identyfikacji elektronicznej oraz tryb notyfikacji krajowego systemu identyfikacji elektronicznej.

Pojęcie identyfikacji elektronicznej (ang. *eID*) można – na podstawie art. 3 pkt 1 i 2 rozporządzenia eIDAS – zdefiniować jako „proces używania danych w postaci elektronicznej identyfikujących osobę, unikalnie reprezentujących osobę fizyczną lub prawną, lub osobę fizyczną reprezentującą osobę prawną"[41], umożliwiających rozpoznanie podmiotu, następujące za pośrednictwem środka identyfikacji elektronicznej, który „oznacza materialną bądź niematerialną jednostkę zawierającą dane identyfikujące osobę i używaną do celów uwierzytelniania dla usługi

[38] M. Kielar, A. Romaszewski, W. Trąbka, K. Gajda, *Warunki wprowadzenia powszechnego systemu identyfikacji elektronicznej i uwierzytelniania w systemie informacyjnym opieki zdrowotnej*, „Zeszyt Naukowy Wyższej Szkoły Zarządzania i Bankowości w Krakowie" 2017/44, s. 27.

[39] M. Kielar, A. Romaszewski, W. Trąbka, K. Gajda, *Warunki...*, s. 27; S. Jakubowski, A. Romaszewski, W. Trąbka, *Identyfikacja i uwierzytelnianie podmiotów oraz dokumentów elektronicznych w ochronie zdrowia jako niezbędne atrybuty bezpieczeństwa danych i informacji w ochronie zdrowia*, „Zeszyt Naukowy Wyższej Szkoły Zarządzania i Bankowości w Krakowie" 2018/49, s. 68.

[40] M. Kielar, A. Romaszewski, W. Trąbka, K. Gajda, *Warunki...*, s. 27.

[41] Na temat definicji osoby prawnej w rozporządzeniu eIDAS zob. komentarz do art. 4 u.u.z.i.

online". Pojęcie to jest nowe; zostało wprowadzone do prawa UE i polskiego porządku prawnego przez wspomniany akt unijny. Najogólniej rzecz ujmując, identyfikacja elektroniczna powinna być rozumiana jako deklaracja (wskazanie) tożsamości, zaprezentowanie unikalnej cechy identyfikującej osobę (lub rzeczy), a zatem elektroniczne „przedstawienie się"[42].

Celem identyfikacji elektronicznej – w świetle rozporządzenia eIDAS – jest między innymi zapewnienie posiadaczowi środka identyfikacji elektronicznej, wydanego w jednym kraju członkowskim UE, możliwości skorzystania z publicznych usług online we własnym państwie oraz w innych krajach członkowskich[43].

11. Identyfikacja elektroniczna stanowi pierwszy etap (zwykle trójetapowej) procedury, którą można określić jako „identyfikacja i uwierzytelnienie"[44]. Drugim etapem tej procedury jest uwierzytelnienie (ang. *authentication*), stanowiące potwierdzenie autentyczności zadeklarowanego wcześniej identyfikatora i prawidłowości identyfikacji (a następnie tożsamości)[45]. Zgodnie z art. 3 pkt 5 rozporządzenia eIDAS „uwierzytelnienie" oznacza „proces elektroniczny umożliwiający identyfikację elektroniczną osoby fizycznej lub prawnej lub potwierdzenie pochodzenia oraz integralności weryfikowanych danych w postaci elektronicznej". Uwierzytelnienie to zatem weryfikacja (udowodnienie) zadeklarowanej tożsamości elektronicznej. Jako przykład uwierzytelnienia można wymienić między innymi porównanie hasła wprowadzonego z hasłem przypisanym do indywidualnego loginu osoby uprawnionej do korzystania z danego systemu lub zbioru danych w bazie[46] czy porównanie

[42] A. Monarcha-Matlak, *Usługi...*, s. 157.
[43] Rządowy projekt ustawy o usługach zaufania..., s. 87.
[44] A. Monarcha-Matlak, *Usługi...*, s. 157.
[45] A. Monarcha-Matlak, *Usługi...*, s. 157.
[46] R. Lewandowski, *Alternatywne narzędzia zdalnej identyfikacji*, „Przegląd Bezpieczeństwa Wewnętrznego" 2021/25, s. 90.

przekazywanych danych biometrycznych z danymi przyporządkowanymi do wskazanej tożsamości[47].

Wyłącznie pozytywny wynik uwierzytelniania pozwala na przejście do trzeciego etapu opisywanego procesu, czyli autoryzacji (ang. *authorization*). Najogólniej rzecz ujmując, autoryzacja polega na weryfikacji, czy użytkownik jest uprawniony do wykonania określonej operacji (np. zlecenia transakcji przelewu) lub korzystania z danego zasobu, a jeżeli tak, to w jakim zakresie[48]. Ponieważ celem autoryzacji jest kontrola dostępu, następuje ona po uwierzytelnieniu[49]. Na gruncie prawa polskiego pojęcie autoryzacji definiuje art. 3 pkt 27 u.i.d.p. Jest ono rozumiane dwojako:

1) jako przydzielenie osobie fizycznej lub prawnej, uprawnień w systemie teleinformatycznym po jej pozytywnym uwierzytelnieniu w tym systemie,
2) jako potwierdzenie woli realizacji czynności w postaci elektronicznej przez uwierzytelnionego użytkownika za pomocą dodatkowych danych (np. ostateczne zatwierdzenie chęci podpisania podania lub wniosku w postaci elektronicznej za pomocą jednorazowego kodu operacji tzw. *OTP*, ang. *one time password*).

Znaczenie pojęcia autoryzacji jest zatem zależne od kontekstu jego użycia.

12. Zgodnie z treścią art. 1 ust. 1 pkt 1 u.u.z.i. komentowana ustawa określa krajową infrastrukturę zaufania (dalej jako KIZ). Przepis art. 2 pkt 1 u.u.z.i. stanowi, że KIZ obejmuje rejestr dostawców usług zaufania, zaufaną listę i narodowe centrum certyfikacji (NCCert). Szerzej na ten temat zob. komentarz do art. 2 u.u.z.i.

---

47 R. Lewandowski, *Alternatywne...*, s. 90.

48 A. Monarcha-Matlak, *Usługi...*, s. 157.

49 R. Lewandowski, *Alternatywne...*, s. 90. W świetle art. 3 pkt 5 rozporządzenia eIDAS uwierzytelnianie oznacza proces elektroniczny, który umożliwia identyfikację elektroniczną osoby fizycznej lub prawnej lub potwierdzenie pochodzenia oraz integralności weryfikowanych danych w postaci elektronicznej.

13. Pojęcie dostawcy usługi zaufania – w tym kwalifikowanego dostawy usług zaufania – omówiono w komentarzu do art. 4 u.u.z.i. Na temat działalności dostawców usług zaufania, w tym zawieszania certyfikatów podpisów elektronicznych i pieczęci elektronicznych (art. 1 ust. 1 pkt 2 u.u.z.i.), zob. komentarz do art. 7 u.u.z.i. i rozdziału 3 komentowanej ustawy.

14. Na temat istoty i trybu notyfikacji krajowego systemu identyfikacji elektronicznej (art. 1 ust. 1 pkt 3 u.u.z.i.) zob. w szczególności komentarz do art. 24 i art. 26 u.u.z.i.

15. Zasady nadzoru, organy nadzoru nad dostawcami usług zaufania oraz środki nadzorcze zostały omówione w komentarzach do przepisów rozdziału 5 (art. 27–39 u.u.z.i.).

16. Pojęcie i strukturę „krajowego schematu identyfikacji elektronicznej" oraz nadzoru nad krajowym schematem identyfikacji elektronicznej przedstawiono w komentarzu do rozdziału 4 (art. 21a–26 u.u.z.i.).

ROZDZIAŁ 2

Krajowa infrastruktura zaufania

Art. 2. [Krajowa infrastruktura zaufania; Rejestr, zaufana lista; NCCert]

Minister właściwy do spraw informatyzacji zapewnia funkcjonowanie krajowej infrastruktury zaufania, która obejmuje:

1) **rejestr dostawców usług zaufania, zwany dalej „rejestrem";**
2) **zaufaną listę;**
3) **narodowe centrum certyfikacji.**

1. Komentowany przepis określa strukturę krajowej infrastruktury zaufania oraz podmiot zapewniający jej funkcjonowanie. Jest nim minister właściwy do spraw informatyzacji.

2. Infrastruktura ujmowana jest najogólniej jako zespół urządzeń i instytucji świadczących usługi, bez których nie byłoby możliwe funkcjonowanie ani rozwój określonego systemu bądź jego fragmentu[50]. Rozu-

[50] Por. M. Ratajczak, *Infrastruktura w gospodarce rynkowej*, Poznań 1999, s. 11.

mienie pojęcia krajowej infrastruktury zaufania przyjęte w ustawie nie odbiega od jego znaczenia przyjętego w języku powszechnym.

Krajowa infrastruktura zaufania obejmuje trzy elementy: rejestr dostawców usług zaufania (dalej jako „Rejestr"), zaufaną listę i NCCert. Krajowa infrastruktura zaufania jest rozwiązaniem pozwalającym z jednej strony na bezpieczny rozwój usług zaufania na rynku polskim, a z drugiej na korzystanie z usług zaufania przez obywateli państw członkowskich Unii Europejskiej[51]. Z technicznego punktu widzenia KIZ przypomina typową infrastrukturę klucza publicznego (ang. *public key infrastructure*, *PKI*), która umożliwia optymalne zarządzanie certyfikatami cyfrowymi[52]. Najistotniejszym elementem infrastruktury klucza publicznego jest centralna instytucja (inaczej urząd certyfikacji, ang. *certification authority*, *CA*), którego rolę pełni NCCert. Instytucja ta wydaje certyfikaty poszczególnym podmiotom (w przypadku KIZ są to dostawcy usług zaufania), a podmioty te wydają certyfikaty swoim klientom (użytkownikom, obywatelom)[53]. Konstrukcja KIZ powoduje, że „wystarczy zaufać NCCert, ponieważ każdy certyfikat wydany klientowi końcowemu jest wydawany przez podmiot, któremu zaufał wcześniej NCCert. Taka hierarchia weryfikacji certyfikatów jest nazywana łańcuchem zaufania (ang. *chain of trust*) lub ścieżką certyfikacji"[54].

3. Zgodnie z art. 2 pkt 1 u.u.z.i. elementem krajowej infrastruktury zaufania jest Rejestr. Ma on postać elektroniczną, jest jawny i każdy ma prawo dostępu do danych w nim zawartych. Wpisuje się do niego dostawców usług zaufania, którzy mają siedzibę lub oddział na terytorium Polski, oraz usługi zaufania przez nich świadczone. Szerzej na temat Rejestru zob. komentarze do art. 3–8 i 11 u.u.z.i.

---

51 W. Wodo, D. Rybak, P. Błaśkiewicz, *Analiza ekosystemu tożsamości cyfrowej w Polsce, stopnia jego wdrożenia i zastosowanie dowodów osobistych z warstwą elektroniczną*, Wrocław 2023, s. 16.

52 W. Wodo, D. Rybak, P. Błaśkiewicz, *Analiza...*, s. 37.

53 W. Wodo, D. Rybak, P. Błaśkiewicz, *Analiza...*, s. 37.

54 W. Wodo, D. Rybak, P. Błaśkiewicz, *Analiza...*, s. 37.

4. Zgodnie z art. 2 pkt 2 u.u.z.i. immanentnym elementem krajowej infrastruktury zaufania jest zaufana lista. W świetle motywu 46 rozporządzenia eIDAS zaufane listy (ang. *trusted lists*) są podstawowym elementem procesu budowania zaufania wśród operatorów rynku wewnętrznego, ponieważ wskazują na kwalifikowany (lub niekwalifikowany) status dostawcy usługi. Obowiązek prowadzenia zaufanej listy wynika wprost z rozporządzenia eIDAS. Przepis art. 22 rozporządzenia eIDAS wskazuje, że każde państwo członkowskie powinno prowadzić i publikować zaufane listy, zawierające informacje o kwalifikowanych dostawcach usług zaufania, za które jest odpowiedzialne, wraz z informacjami o świadczonych przez tych dostawców kwalifikowanych usługach zaufania w postaci dostosowanej do automatycznego przetwarzania. Ponadto państwa członkowskie przekazują Komisji Europejskiej informacje o podmiocie odpowiedzialnym za sporządzenie i opublikowanie zaufanej listy wraz z informacjami szczegółowymi dotyczącymi miejsca jej publikacji (art. 1 decyzji wykonawczej Komisji (UE) 2015/1505 z 8.09.2015 r. ustanawiającej specyfikacje techniczne i formaty dotyczące zaufanych list zgodnie z art. 22 ust. 5 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.Urz. UE L 235, s. 26). Państwa członkowskie mogą umieścić w zaufanych listach informacje na temat dostawców niekwalifikowanych usług zaufania wraz z informacjami dotyczącymi świadczonych przez nich niekwalifikowanych usług. W takiej zbiorczej liście precyzuje się, którzy dostawcy usług zaufania nie są dostawcami kwalifikowanymi oraz które świadczone przez nich usługi zaufania nie są kwalifikowane (art. 2 decyzji wykonawczej 2015/1505)[55].

Prowadzenie zaufanej listy odbywa się zgodnie z wymaganiami określonymi w decyzji wykonawczej 2015/1505. Każde państwo członkowskie prowadzi własne „krajowe" zaufane listy[56]. Zaufane listy państw członkowskich zawierają co najmniej informacje określone w art. 1 i 2 decyzji

[55] Ł. Goździaszek, *Identyfikacja...*, komentarz do art. 22 rozporządzenia eIDAS.
[56] Zob.: https://eidas.ec.europa.eu/efda/tl-browser/#/screen/home (dostęp: 6.01.2024 r.).

wykonawczej 2015/1505. Na tych listach znajdują się zarówno aktualne, jak i archiwalne informacje, w tym daty umieszczenia dostawcy usług zaufania na zaufanych listach, a także informacje o statusie usług zaufania na nich wymienionych.

Krajową zaufaną listę prowadzi – na mocy upoważnienia ministra właściwego do spraw informatyzacji – NCCert (art. 5 ust. 2 u.u.z.i.). Decyzja o wpisie do Rejestru kwalifikowanych dostawców usług zaufania jest podstawą do wydania certyfikatu przez NCCert oraz dokonania wpisu na zaufaną listę i oznacza nadanie statusu kwalifikowanego dostawcy usług zaufania lub świadczonej przez niego usłudze (tak art. 5 ust. 1 u.u.z.i.). Polska zaufana lista publikowana jest na stronie NCCert[57] i zawiera informacje dotyczące kwalifikowanych dostawców usług zaufania wraz z informacjami o ich usługach. Zgodnie z art. 8 ust. 5 u.u.z.i. decyzja o wykreśleniu z Rejestru kwalifikowanego dostawcy usług zaufania jest podstawą wykreślenia go również z zaufanej listy oraz może być podstawą do unieważnienia certyfikatu. Zaufana lista jest więc niezwykle ważnym elementem budowania zaufania na europejskim rynku usług zaufania, umożliwia bowiem ustalenie statusu kwalifikowanych dostawców[58].

5. Narodowe centrum certyfikacji (NCCert) to system informatyczny Narodowego Banku Polskiego, stworzony w celu realizacji zadań powierzonych NBP przez ministra właściwego do spraw informatyzacji, zgodnie z ustawą o usługach zaufania oraz identyfikacji elektronicznej[59]. Pełni on rolę głównego urzędu certyfikacji w polskiej infrastrukturze zaufania[60], a odpowiada – przede wszystkim – za wytwarzanie, wydawanie i unieważnianie certyfikatów dostawców usług zaufania. Narodowe centrum certyfikacji tworzy i wydaje kwalifikowanym dostawcom usług zaufania certyfikaty służące do weryfikacji zaawansowanych podpisów

[57] Dostępna pod adresem: https://www.nccert.pl
[58] Szerzej M. Marucha-Jaworska, *Rozporządzenie...*, s. 158 i n.
[59] Zob.: https://www.nccert.pl (dostęp: 6.01.2024 r.).
[60] Określenie to pochodzi z Polityki Certyfikacji NCCert (zob. pkt 1.1. i 1.4.2. Polityki Certyfikacji NCCert).

elektronicznych lub pieczęci elektronicznych oraz certyfikatów służących do weryfikacji innych usług zaufania świadczonych przez kwalifikowanych dostawców, publikuje certyfikaty i listy unieważnionych certyfikatów, tworzy dane do opatrywania pieczęcią elektroniczną certyfikatów oraz certyfikatów do weryfikacji tych pieczęci (szerzej na temat NCCert zob. komentarz do art. 10 u.u.z.i.). Działalność tego podmiotu jest nie tylko ważnym elementem KIZ, ale i fundamentem zapewnienia skutecznego nadzoru nad dostawcami usług zaufania.

Zgodnie z art. 11 ust. 1 u.u.z.i. na mocy upoważnienia z 27.10.2016 r. ministra właściwego do spraw informatyzacji (wydanego na wniosek Prezesa NBP) do zadań NCCert należy (jak wspomniano już wyżej) prowadzenie zaufanej listy w Polsce (ang. *TSL*) oraz Rejestru. Zob. szerzej komentarz do art. 11 u.u.z.i.

6. Minister Cyfryzacji na podstawie upoważnienia ustawowego zawartego w art. 12 u.u.z.i. wydał 5.10.2016 r. rozporządzenie w sprawie krajowej infrastruktury zaufania, określające:

1) szczegółową treść wpisów w Rejestrze oraz sposób ich dokonywania;
2) tryb wydawania i unieważniania certyfikatów dostawcy usług zaufania oraz certyfikatów NCCert;
3) wymagania dla Polityki Certyfikacji NCCert;
4) wymagania organizacyjno-techniczne i bezpieczeństwa krajowej infrastruktury zaufania.

Rozporządzenie określa szczegółową treść wpisów w Rejestrze (§ 3 r.k.i.z.) oraz sposób ich dokonywania, tryb wydawania i unieważniania certyfikatów dostawcy usług zaufania oraz certyfikatów NCCert (§ 4–6 r.k.i.z.), jak również wymagania dla Polityki Certyfikacji NCCert. Zgodnie z przepisami tego rozporządzenia wpis do Rejestru dokonywany jest w postaci elektronicznej przez wprowadzenie informacji zawartych w decyzji o wpisie albo zgłoszeniu przesłanym przez dostawcę usług zaufania. Treść wpisu powinna obejmować informacje wskazane w § 3 r.k.i.z. Wydanie certyfikatu dostawcy usług zaufania następuje z urzędu, natomiast jego unieważnienie na wniosek ministra właściwego

do spraw informatyzacji (w terminie określonym we wniosku). Na wniosek tego ministra następuje także wydanie i unieważnienie certyfikatu NCCert. W rozporządzeniu w sprawie krajowej infrastruktury zaufania uregulowano również terminy na dokonanie wpisu do Rejestru oraz na wydanie certyfikatu dostawcy usług zaufania.

W § 7 r.k.i.z. określone zostały także wymagania dla Polityki Certyfikacji NCCert. Powołana polityka podlega uzgodnieniu z kwalifikowanymi dostawcami usług zaufania. Zgodnie z § 8 r.k.i.z. NCCert oraz Rejestr muszą spełniać wymagania organizacyjno-techniczne oraz wymagania bezpieczeństwa określone w normie ETSI EN 319 401 i w normie ETSI EN 319 411.

Art. 3. [Rejestr dostawców usług zaufania]

1. Rejestr jest prowadzony w postaci elektronicznej.
2. Rejestr jest jawny. Każdy ma prawo dostępu do danych zawartych w rejestrze.
3. Do rejestru wpisuje się dostawców usług zaufania, którzy mają siedzibę lub oddział na terytorium Rzeczypospolitej Polskiej, oraz usługi zaufania świadczone przez tych dostawców.
4. Do rejestru wpisuje się:

1) **imię i nazwisko lub firmę (nazwę) dostawcy usług zaufania;**
2) **adres siedziby i miejsca wykonywania działalności;**
3) **numer w Krajowym Rejestrze Sądowym – w przypadku dostawców usług zaufania podlegających wpisowi do tego rejestru;**
4) **numer identyfikacji podatkowej;**
5) **nazwę polityki świadczenia usług;**
6) **rodzaj świadczonych usług zaufania;**
7) **datę rozpoczęcia świadczenia usługi zaufania;**
8) **datę zakończenia świadczenia usługi zaufania;**
9) **informację o wystawionych certyfikatach, o których mowa w art. 10 ust. 1 pkt 1;**

10) nazwę i adres zakładu ubezpieczeń, z którym dostawca usług zaufania zawarł umowę ubezpieczenia, okres, na jaki umowa ta została zawarta, oraz sumę ubezpieczenia;
11) informacje o zamiarze zaprzestania prowadzenia działalności w zakresie świadczenia usług zaufania lub zamiarze ograniczenia zakresu świadczonych usług zaufania;
12) informacje o otwarciu likwidacji dostawcy usług zaufania oraz datę jego likwidacji;
13) informacje o ogłoszeniu upadłości dostawcy usług zaufania lub oddaleniu wniosku o ogłoszenie upadłości z przyczyn wskazanych w art. 13 ustawy z dnia 28 lutego 2003 r. – Prawo upadłościowe (Dz. U. z 2020 r. poz. 1228 i 2320 oraz z 2021 r. poz. 1080, 1177 i 1598) oraz datę zakończenia postępowania upadłościowego;
14) datę wykreślenia z rejestru dostawcy usług zaufania.

1. Rejestr jest jednym z elementów krajowej infrastruktury zaufania (szerzej na temat KIZ zob. w komentarzu do art. 2 u.u.z.i.). Za jego funkcjonowanie – zgodnie z art. 2 pkt 1 u.u.z.i. – odpowiada minister właściwy do spraw informatyzacji. W związku z jego prowadzeniem na ministrze ciążą obowiązki określone nie tylko w komentowanej ustawie, lecz także w ustawie o informatyzacji działalności podmiotów realizujących zadania publiczne (por. w szczególności art. 14 u.i.d.p.).

Rejestr ten jest centralnym rejestrem publicznym (zob. art. 3 pkt 5 u.i.d.p.) i powinien spełniać wymagania stawiane tego typu rejestrom[61]. Wpisuje się do niego dostawców usług zaufania, którzy mają siedzibę lub oddział na terytorium Rzeczypospolitej Polskiej, oraz usługi zaufania świadczone przez tych dostawców. Na gruncie prawa polskiego siedzibą osoby prawnej jest, co do zasady, miejscowość określona w jej statucie lub ustawie, na podstawie którego powstaje osoba prawna. W braku od-

[61] Na temat cech rejestru centralnego m.in. J. Dobkowski, *Rejestry publiczne o charakterze personalnym prowadzone w systemie teleinformatycznym i administracyjne prawo dowodowe*, „Casus" 2018/91, s. 63.

miennych postanowień, zgodnie z dyspozycją art. 41 k.c., siedzibą osoby prawnej jest miejscowość, w której ma siedzibę organ zarządzający tą osobą prawną (art. 41 k.c.). Każda osoba prawna ma zatem jedną siedzibę, a jej zmiana wymaga odpowiednio zmiany statutu, ustawy lub siedziby organu zarządzającego[62]. Siedzibą jest przy tym skonkretyzowana miejscowość, a nie jej adres (chyba że co innego wynika z przepisu szczególnego). Siedziba osoby prawnej zarejestrowanej w Polsce powinna być usytuowana na terytorium Rzeczypospolitej Polskiej[63].

Rejestr ma charakter mieszany: zasadniczo jest rejestrem podmiotowym (personalnym, tj. pełniącym funkcję identyfikacyjną w odniesieniu do określonych – wskazanych w omawianej ustawie – osób i jednostek organizacyjnych)[64], a w części rejestrem przedmiotowym (tj. ujawniającym usługi zaufania świadczone przez dostawców tych usług).

Zgodnie z treścią komentowanego artykułu Rejestr jest prowadzony w postaci elektronicznej i jest jawny. Podzielony jest na część obejmującą kwalifikowane usługi zaufania i część dotyczącą świadczenia niekwalifikowanych usług zaufania. Każdy ma prawo dostępu do danych w nim zawartych. Odbywa się to w formie wglądu z możliwością bieżącego podglądu danych w nim zamieszczonych[65]. W realiach krajowych Rejestr jest prowadzony przez NBP i można go przeglądać na stronie internetowej NCCert[66]. Wpisy w Rejestrze domyślnie uszeregowane są według dat uzyskania wpisu do rejestru – w kolejności od najwcześniejszego, ze wskazaniem daty i czasu dokonania wpisu.

2. W świetle art. 3 ust. 4 u.u.z.i. do Rejestru wpisuje się dane enumeratywnie wymienione w tym przepisie. Są one odzwierciedleniem danych, jakie

---

62 W. Czuchwicki, komentarz do art. 41 k.c. [w:] *Kodeks cywilny. Komentarz*, red. M. Balwicka-Szczyrba, A. Sylwestrzak, LEX 2023.

63 P. Nazaruk, komentarz do art. 41 k.c. [w:] *Kodeks cywilny. Komentarz*, red. J. Ciszewski, P. Nazaruk, LEX 2023, zob też cyt. tam literaturę.

64 J. Dobkowski, *Rejestry...*, s. 63 i cyt. tam literatura.

65 Na temat dostępu do rejestrów personalnych zob. szerzej J. Dobkowski, *Rejestry...*, s. 63.

66 Zob.: https://www.nccert.pl/uslugi.htm (dostęp: 6.01.2024 r.).

należy podać we wniosku o wpis do Rejestru w części dotyczącej kwalifikowanych dostawców usług zaufania lub kwalifikowanej usługi zaufania (zob. art. 4 ust. 2 u.u.z.i.) albo w zgłoszeniu w zakresie odnoszącym się do niekwalifikowanego dostawcy usług zaufania lub niekwalifikowanej usługi zaufania (art. 6 ust. 2 u.u.z.i.). Do Rejestru zgodnie z art. 3 ust. 4 u.u.z.i. wpisuje się: imię i nazwisko lub firmę (nazwę) dostawcy usług zaufania, w zależności od formy prowadzonej przez niego działalności; adres siedziby i miejsca wykonywania działalności; numer w KRS – w przypadku dostawców usług zaufania podlegających wpisowi do tego rejestru; numer identyfikacji podatkowej. Ponadto wpisuje się nazwę polityki świadczenia usług. Zgodnie z art. 19 ust. 1 u.u.z.i. dostawca usług zaufania jest obowiązany posiadać politykę świadczenia usługi. Najogólniej ujmując, polityka świadczenia usługi jest ważnym narzędziem zarządzania usługami w różnego rodzaju podmiotach i pomaga zapewnić między innymi spójność, jakość i przejrzystość procesu ich świadczenia. Stosownie zaś do art. 19 ust. 2 u.u.z.i. polityka świadczenia usługi stanowi nazwany zestaw reguł, w szczególności takich jak polityka certyfikacji, określający zasady świadczenia usługi, odpowiedzialność stron, zasady postępowania z danymi i mający zastosowanie do określonego kręgu podmiotów lub zastosowań, o wspólnych dla tego kręgu wymaganiach bezpieczeństwa, opracowywany na podstawie norm lub standardów określających wymagania dla polityk świadczenia usług. Polityka świadczenia usługi została szerzej omówiona w komentarzu do art. 19 u.u.z.i.

Rejestr zawiera także informacje: o rodzaju świadczonych usług zaufania, dacie rozpoczęcia świadczenia usługi zaufania, dacie zakończenia świadczenia usługi zaufania, informację o wystawionych certyfikatach, o których mowa w art. 10 ust. 1 pkt 1 u.u.z.i., czyli certyfikatach wydawanych przez NCCert kwalifikowanym dostawcom usług zaufania służącym do weryfikacji zaawansowanych podpisów elektronicznych lub pieczęci elektronicznych, oraz certyfikatach służących do weryfikacji innych usług zaufania świadczonych przez kwalifikowanych dostawców. W Rejestrze podaje się: nazwę i adres zakładu ubezpieczeń, z którym dostawca usług zaufania zawarł umowę ubezpieczenia, okres, na jaki

umowa ta została zawarta, oraz sumę ubezpieczenia, informacje o zamiarze zaprzestania prowadzenia działalności w zakresie świadczenia usług zaufania lub zamiarze ograniczenia zakresu świadczonych usług zaufania, informacje o otwarciu likwidacji dostawcy usług zaufania oraz datę jego likwidacji, informacje o ogłoszeniu upadłości dostawcy usług zaufania lub oddaleniu wniosku o ogłoszenie upadłości z przyczyn wskazanych w art. 13 pr. upad., a także datę zakończenia postępowania upadłościowego.

3. Ustawa o usługach zaufania oraz identyfikacji elektronicznej nie uprawnia wprost ministra właściwego do spraw informatyzacji do wydania decyzji administracyjnej w sprawie dokonania zmian w Rejestrze, poprzestając na wskazaniu, że wpis do Rejestru, odmowa wpisu do Rejestru oraz wykreślenie z Rejestru następują w drodze decyzji administracyjnej. Komentowany akt normatywny odnosi się do zmiany danych wpisanych do Rejestru wyłącznie w art. 7 u.u.z.i. Przepis ten w ust. 1 przewiduje, że dostawca usług zaufania wpisany do Rejestru powinien poinformować ministra właściwego do spraw informatyzacji o każdej zmianie danych wpisanych do Rejestru, w terminie 14 dni od zmiany tych danych. Zasadna jest teza, że zarówno dokonanie wpisu, jak i zmiana wpisu dotyczące kompetencji ministra właściwego do spraw informatyzacji jako organu nadzoru prowadzącego Rejestr powinny być dokonywane w formie decyzji administracyjnej. Skoro bowiem organ jest uprawniony do odmowy wpisu kwalifikowanej usługi zaufania lub kwalifikowanego dostawcy usługi zaufania do Rejestru oraz ich wykreślenia, to tym bardziej może odmówić zmian wpisu w Rejestrze w formie decyzji administracyjnej[67]. Założenie, że ustawodawca celowo nie przewidział decyzji w przedmiocie wpisu aktualizującego do Rejestru (ponieważ nie pełni ona żadnej funkcji reglamentacyjnej), jest sprzeczne z wykładnią systemową przepisów ustawy o usługach zaufania oraz identyfikacji elektronicznej. Pamiętać bowiem należy, że zmiana niektórych danych zawartych w Rejestrze, jak np. zmiana polityki certyfikacji, wiąże się z określonymi uprawnieniami i obowiązkami różnych podmiotów. Wydanie

[67] Por. wyrok WSA w Warszawie z 22.04.2021 r., VII SA/Wa 2089/20, LEX nr 3184763.

decyzji administracyjnej w sprawie aktualizacji danych jest zdaniem autorów zasadne o tyle, o ile zakres zmian nie dotyczy czysto formalnych kwestii, niewpływających znacząco na świadczone dotychczas usługi zaufania. Wówczas dostawca usługi realizuje obowiązek informacyjny, a organ nadzoru przyjmuje to zawiadomienie bez konieczności wydawania decyzji. Taka systemowa wykładnia przepisów ustawy pozostaje w zgodzie ze sposobem funkcjonowania organów rejestracyjnych na tle uregulowań innych aktów prawa (np. w ustawie z 6.03.2018 r. o Centralnej Ewidencji i Informacji o Działalności Gospodarczej i Punkcie Informacji dla Przedsiębiorcy, Dz.U. z 2022 r. poz. 541 ze zm.). Mając na uwadze wątpliwości powstające na tym tle, należałoby postulować doprecyzowanie przepisów i wyraźne wskazanie uprawnienia do wydawania decyzji administracyjnej w tym zakresie przez organ nadzoru.

Szczegółowa treść oraz sposób dokonywania wpisów w Rejestrze zostały uregulowane w rozporządzeniu w sprawie krajowej infrastruktury zaufania na podstawie upoważnienia ustawowego zawartego w art. 12 u.u.z.i.

Art. 4. [Wpis do Rejestru dostawcy usług zaufania lub kwalifikowanej usługi zaufania]

1. Wpis do rejestru:

1) **dostawcy usług zaufania, który zamierza świadczyć kwalifikowane usługi zaufania, lub**
2) **kwalifikowanej usługi zaufania**

– następuje na wniosek dostawcy usług zaufania.

2. Wniosek o wpis, o którym mowa w ust. 1, zawiera dane i informacje, o których mowa w art. 3 ust. 4 pkt 1–7.

3. Minister właściwy do spraw informatyzacji udostępnia w Biuletynie Informacji Publicznej formularz wniosku o wpis, o którym mowa w ust. 1.

4. Do wniosku o wpis, o którym mowa w ust. 1, dołącza się, w postaci elektronicznej: