



Prezes Rady Ministrów

Mateusz Morawiecki

Warszawa, dnia /elektroniczny znacznik czasu/

RM-0610-121-23
UD7

Pan Szymon HOŁOWNIA
Marszałek Sejmu

Szanowny Panie Marszałku,

na podstawie art. 118 ust. 1 Konstytucji Rzeczypospolitej Polskiej przedstawiam Sejmowi projekt ustawy o zmianie niektórych ustaw w celu rozwoju usług cyfrowych. Do prezentowania stanowiska Rządu w tej sprawie w toku prac parlamentarnych został upoważniony Minister Rozwoju i Technologii.

Z poważaniem
Mateusz Morawiecki
/podpisano kwalifikowanym podpisem elektronicznym/

Do wiadomości:
wnioskodawca

U S T A W A

z dnia

o zmianie niektórych ustaw w celu rozwoju usług cyfrowych¹⁾

Art. 1. W ustawie z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego (Dz. U. z 2023 r. poz. 775 i 803) w art. 33 dodaje się § 5 i 6 w brzmieniu:

„§ 5. W przypadku gdy strona udzieliła pełnomocnictwa, o którym mowa w art. 19ac ust. 2 pkt 2 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne, z wykorzystaniem Rejestru Pełnomocnictw Elektronicznych, o którym mowa w art. 19ac ust. 1 tej ustawy, organ, po podaniu przez pełnomocnika imienia i nazwiska lub numeru PESEL pełnomocnika lub mocodawcy, dokonuje weryfikacji istnienia pełnomocnictwa, jego ważności oraz zakresu upoważnienia do występowania w imieniu strony w tym rejestrze oraz zamieszcza w aktach adnotację o dokonaniu tej weryfikacji.

§ 6. W przypadku, o którym mowa w § 5, organ nie może żądać dostarczenia przez pełnomocnika dokumentu pełnomocnictwa udzielonego na piśmie.”.

Art. 2. W ustawie z dnia 21 sierpnia 1997 r. o gospodarce nieruchomościami (Dz. U. z 2023 r. poz. 344, z późn. zm.²⁾) wprowadza się następujące zmiany:

1) w art. 156 ust. 1 otrzymuje brzmienie:

„1. Rzecznawca majątkowy sporządza opinię o wartości nieruchomości w formie operatu szacunkowego. Operat szacunkowy sporządza się w postaci papierowej lub elektronicznej.”;

2) w art. 192 dodaje się ust. 3 w brzmieniu:

„3. Świadcstwo jest wydawane w postaci spersonalizowanej dwustronnej karty identyfikacyjnej, zawierającej fotografię rzeczoznawcy majątkowego. W przypadku osób posiadających obywatelstwo polskie fotografię pobiera się z Rejestru Dowodów

¹⁾ Niniejszą ustawą zmienia się ustawy: ustawę z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego, ustawę z dnia 21 sierpnia 1997 r. o gospodarce nieruchomościami, ustawę z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne, ustawę z dnia 6 sierpnia 2010 r. o dowodach osobistych, ustawę z dnia 24 września 2010 r. o ewidencji ludności, ustawę z dnia 23 listopada 2012 r. – Prawo pocztowe, ustawę z dnia 18 listopada 2020 r. o doręczeniach elektronicznych oraz ustawę z dnia 26 maja 2023 r. o aplikacji mObywatel.

²⁾ Zmiany tekstu jednolitego niniejszej ustawy zostały ogłoszone w Dz. U. z 2023 r. poz. 1113, 1463, 1506, 1688, 1762, 1906 i 2029.

Osobistych, o którym mowa w ustawie z dnia 6 sierpnia 2010 r. o dowodach osobistych (Dz. U. z 2022 r. poz. 671 oraz z 2023 r. poz. 1234, 1941 i). W przypadku tych osób świadectwo może być również wydane w postaci dokumentu mobilnego, o którym mowa w art. 2 pkt 7 ustawy z dnia 26 maja 2023 r. o aplikacji mObywatel (Dz. U. poz. 1234 i).”;

3) w art. 197 pkt 3 otrzymuje brzmienie:

„3) wzory dokumentów związanych z nadaniem uprawnień zawodowych w zakresie szacowania nieruchomości, w szczególności świadectwa nadania tych uprawnień, a także warunki i tryb wydawania tych dokumentów;”.

Art. 3. W ustawie z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2023 r. poz. 57, 1123, 1234 i 1703) wprowadza się następujące zmiany:

1) po art. 12a dodaje się art. 12aa–12ad w brzmieniu:

„Art. 12aa. 1. Minister właściwy do spraw informatyzacji opracowuje dokument o charakterze strategicznym w dziedzinie informatyzacji państwa, zwany dalej „strategią”, uwzględniając w szczególności:

- 1) aktualny stan informatyzacji państwa;
- 2) otoczenie strategiczne;
- 3) wizję informatyzacji państwa;
- 4) cele i priorytety informatyzacji państwa;
- 5) środki służące realizacji celów strategii;
- 6) sposoby i zasady współpracy z podmiotami, których dotyczy proces informatyzacji;
- 7) możliwości finansowania projektowanych działań.

2. Projekt strategii opracowuje minister właściwy do spraw informatyzacji we współpracy z innymi członkami Rady Ministrów.

3. Rada Ministrów, na wniosek ministra właściwego do spraw informatyzacji, przyjmuje strategię w drodze uchwały.

4. Strategia jest przyjmowana na okres dziesięcioletni i może być zmieniana w tym okresie.

Art. 12ab. Minister właściwy do spraw informatyzacji we współpracy z członkami Rady Ministrów dokonuje przeglądu strategii co 2 lata.

Art. 12ac. Koordynatorem działań mających na celu realizację strategii jest minister właściwy do spraw informatyzacji.

Art. 12ad. Strategię ogłasza się w Dzienniku Urzędowym Rzeczypospolitej Polskiej „Monitor Polski” oraz udostępnia się w Biuletynie Informacji Publicznej na stronie podmiotowej ministra właściwego do spraw informatyzacji.”;

- 2) uchyla się art. 12b;
- 3) uchyla się art. 15a;
- 4) po art. 19a dodaje się art. 19aa-19ac w brzmieniu:

„Art. 19aa. 1. Podmiot publiczny może udostępniać usługi online dostosowane do potrzeb użytkownika na podstawie danych tego użytkownika, w szczególności danych:

- 1) osobowych użytkownika,
- 2) dotyczących sytuacji prawnej użytkownika lub praw mu przysługujących, umożliwiających identyfikację rzeczy związanej z użytkownikiem
– pobranych z rejestrów publicznych lub systemów teleinformatycznych tego podmiotu.

2. Podmiot publiczny udostępnia dane gromadzone w prowadzonym rejestrze publicznym lub w systemie teleinformatycznym innemu podmiotowi publicznemu lub podmiotowi, o którym mowa w art. 19c ust. 1, wyłącznie na potrzeby usługi online, która jest świadczona na rzecz użytkownika przy wykorzystaniu systemu teleinformatycznego.

3. Udostępnienie danych, o których mowa w ust. 2, następuje:

- 1) po wyrażeniu woli skorzystania z usługi online przez uwierzytelnionego użytkownika, na rzecz którego świadczona jest ta usługa online i którego te dane dotyczą;
- 2) za pośrednictwem usług sieciowych między systemem teleinformatycznym, z którego udostępniane są dane, a systemem teleinformatycznym, przy wykorzystaniu, którego świadczona jest usługa online.

4. Podmioty, o których mowa w ust. 2, zawierają porozumienie określające zasady współpracy, w tym warunki udostępniania danych, o których mowa w ust. 2.

Art. 19ab. 1. Minister właściwy do spraw informatyzacji może udostępniać usługi online przy wykorzystaniu systemów teleinformatycznych tego ministra, w celu wykonywania zadań publicznych przez tego ministra oraz inne podmioty publiczne lub niepubliczne, w tym usługi polegające na:

- 1) zarządzaniu skrzynką doręczeń w rozumieniu ustawy z dnia 18 listopada 2020 r. o doręczeniach elektronicznych (Dz. U. z 2023 r. poz. 285, 1860 i ...);

- 2) zapewnianiu dostępu do konta ePUAP;
- 3) przyjmowaniu i dostępie do pełnomocnictw gromadzonych w Rejestrze Pełnomocnictw Elektronicznych.

2. W zakresie niezbędnym do realizacji usługi online udostępnianej przez ministra właściwego do spraw informatyzacji następuje wymiana informacji między systemami teleinformatycznymi tego ministra a systemem teleinformatycznym podmiotu, na rzecz którego udostępniana jest ta usługa.

3. Podmioty publiczne przekazują ministrowi właściwemu do spraw informatyzacji dane niezbędne do udostępnienia usług online, w tym dane osobowe użytkownika oraz dotyczące jego sytuacji prawnej lub praw mu przysługujących oraz dane dotyczące wiarytelności.

4. Przekazywanie danych na podstawie przepisów ust. 2 i 3 nie narusza przepisów dotyczących tajemnic prawnie chronionych.

5. System teleinformatyczny wykorzystywany do udostępniania usługi online jest przyłączony do węzła krajowego identyfikacji elektronicznej w rozumieniu ustawy z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej (Dz. U. z 2021 r. poz. 1797 oraz z 2023 r. poz. 1234).

6. Udostępnianie usługi online przez ministra właściwego do spraw informatyzacji na rzecz podmiotów niebędących podmiotami publicznymi odbywa się z zachowaniem zasad równego traktowania tych podmiotów. Przepisy ust. 7 i 8 stosuje się odpowiednio.

7. Minister właściwy do spraw informatyzacji może zawierać z innymi podmiotami publicznymi porozumienia określające:

- 1) sposób udostępnienia usług online;
- 2) zakres udostępnianych danych, o których mowa w ust. 3, a także sposób i tryb ich udostępniania.

8. Minister właściwy do spraw informatyzacji może określić ogólne warunki udostępniania usług online.

9. Udostępnianie przez ministra właściwego do spraw informatyzacji usługi online odbywa się na podstawie:

- 1) porozumienia, o którym mowa w ust. 7, albo
- 2) ogólnych warunków, o których mowa w ust. 8.

10. W celu zapewnienia realizacji czynności związanych z obsługą systemów teleinformatycznych w imieniu i na rzecz podmiotu, w tym obsługi spraw związanych z

usługami online, minister właściwy do spraw informatyzacji może utworzyć na wniosek podmiotu w swoim systemie jego konto.

11. Wniosek, o którym mowa w ust. 10, jest składany do ministra właściwego do spraw informatyzacji.

12. Wniosek, o którym mowa w ust. 10, zawiera:

- 1) dane podmiotu, którego konto ma zostać utworzone;
- 2) określenie czynności związanych z obsługą systemów teleinformatycznych realizowanych w imieniu i na rzecz tego podmiotu;
- 3) wskazanie administratora uprawnionego do dokonywania czynności w imieniu i na rzecz podmiotu, w tym nadawania dalszych uprawnień.

Art. 19ac. 1. Minister właściwy do spraw informatyzacji prowadzi przy użyciu systemu teleinformatycznego Rejestr Pełnomocnictw Elektronicznych służący do udzielania przez uwierzytelnionego użytkownika pełnomocnictw elektronicznych osobie fizycznej posiadającej numer PESEL oraz ich gromadzenia.

2. Pełnomocnictwo elektroniczne może obejmować:

- 1) prawo do korzystania z usług online udostępnianych przez ministra właściwego do spraw informatyzacji lub za jego pośrednictwem, w szczególności:
 - a) dostęp do systemu teleinformatycznego wykorzystywanego do udostępniania usług online, w tym ePUAP, wgląd w dane mocodawcy dostępne za pośrednictwem tego systemu oraz zarządzanie skrzynką doręczeń,
 - b) składanie oświadczeń w imieniu i na rzecz mocodawcy w ramach udostępnianych usług online;
- 2) prawo do wykonania czynności przed podmiotem publicznym, o którym mowa w art. 2 ust. 1 pkt 1, 2 i 4–8, z zastrzeżeniem ust. 13, w przypadku zintegrowania systemu teleinformatycznego podmiotu publicznego z rejestrem, o którym mowa w ust. 1;
- 3) pełnomocnictwo pocztowe, o którym mowa w art. 38 ust. 1 ustawy z dnia 23 listopada 2012 r. – Prawo pocztowe (Dz. U. z 2023 r. poz 1640 i);
- 4) inne pełnomocnictwo o treści ustalonej przez mocodawcę, udzielane na podstawie art. 98 ustawy z dnia 23 kwietnia 1964 r. – Kodeks cywilny (Dz. U. z 2023 r. poz. 1610, 1615, 1890 i 1933).

3. Pełnomocnictwo elektroniczne zawiera co najmniej imię, nazwisko, numer PESEL pełnomocnika i mocodawcy oraz zakres upoważnienia.

4. Pełnomocnictwa elektroniczne, o których mowa w ust. 2 pkt 2–4, opatruje się:

- 1) kwalifikowanym podpisem elektronicznym,
- 2) podpisem zaufanym,
- 3) podpisem osobistym albo
- 4) zaawansowaną pieczęcią elektroniczną ministra właściwego do spraw informatyzacji, po uwierzytelnieniu wnioskodawcy z wykorzystaniem certyfikatu podstawowego, o którym mowa w art. 2 pkt 2 ustawy z dnia 26 maja 2023 r. o aplikacji mObywatel.

5. Udzielenie pełnomocnictwa elektronicznego, o którym mowa w ust. 2 pkt 1, następuje po uwierzytelnieniu środkiem identyfikacji elektronicznej wykorzystującym co najmniej dwa czynniki uwierzytelnienia należące do co najmniej dwóch różnych kategorii, o których mowa w przepisach wydanych na podstawie art. 8 ust. 3 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 oraz uchylającego dyrektywę 1999/93/WE (Dz. Urz. UE L 257 z 28.08.2014, str. 73 i Dz. Urz. UE L 333 z 27.12.2022, str. 80).

6. Pełnomocnictwo elektroniczne, o którym mowa w ust. 2 pkt 1, nie upoważnia do dostępu do danych i korzystania z usług online, które zostały udostępnione mocodawcy na podstawie innego pełnomocnictwa.

7. Pełnomocnictwo elektroniczne, o którym mowa w ust. 2 pkt 4:

- 1) nie wywołuje skutków prawnych w postępowaniu prowadzonym przed organem administracji publicznej;
- 2) nie może być udzielone:
 - a) w postępowaniu egzekucyjnym,
 - b) jako pełnomocnictwo procesowe,
 - c) jeżeli do ważności czynności prawnej potrzebna jest szczególna forma.

8. Minister właściwy do spraw informatyzacji na wniosek operatora pocztowego zapewnia możliwość udzielania pełnomocnictw elektronicznych, o których mowa w ust. 2 pkt 3. Treść pełnomocnictwa ustalona jest zgodnie z art. 38 ust. 2 ustawy z dnia 23 listopada 2012 r. – Prawo pocztowe.

9. W przypadku, o którym mowa w ust. 8, minister właściwy do spraw informatyzacji pobiera opłatę należną za to pełnomocnictwo określoną w cenniku usług pocztowych lub w cenniku usług powszechnych operatora pocztowego i przekazuje ją operatorowi pocztowemu.

10. W przypadku, o którym mowa w ust. 8, minister właściwy do spraw informatyzacji oraz operator pocztowy zawierają porozumienie określające zasady współpracy, w tym terminy przekazywania opłaty, o której mowa w ust. 9, oraz sposób weryfikacji liczby udzielonych pełnomocnictw.

11. W przypadku gdy czynność jest związana z usługą online, informacja o udzieleniu pełnomocnictwa elektronicznego, o którym mowa w ust. 2 pkt 2, może być przekazana w ramach tej usługi.

12. Mocodawca może odwołać udzielone pełnomocnictwo elektroniczne w każdym czasie. W przypadku odwołania pełnomocnictwa elektronicznego minister właściwy do spraw informatyzacji oznacza pełnomocnictwo elektroniczne znajdujące się w Rejestrze Pełnomocnictw Elektronicznych adnotacją o jego odwołaniu.

13. W przypadku śmierci mocodawcy lub pełnomocnika minister właściwy do spraw informatyzacji oznacza pełnomocnictwa elektroniczne znajdujące się w Rejestrze Pełnomocnictw Elektronicznych adnotacją o śmierci tej osoby.

14. Minister właściwy do spraw informatyzacji określa listę czynności, w stosunku do których możliwe jest udzielenie pełnomocnictwa elektronicznego, o którym mowa w ust. 2 pkt 2:

- 1) w przypadku czynności realizowanych z wykorzystaniem systemu teleinformatycznego, którego funkcjonowanie zapewnia ten minister, lub
- 2) na wniosek podmiotu publicznego, o którym mowa w art. 2 ust. 1 pkt 1, 2 i 4-8.

15. Minister właściwy do spraw informatyzacji ogłasza w swoim dzienniku urzędowym oraz w Biuletynie Informacji Publicznej na swojej stronie podmiotowej informację o:

- 1) czynnościach, w stosunku do których jest możliwe udzielenie pełnomocnictwa elektronicznego, o którym mowa w ust. 2 pkt 2;
- 2) podmiotach posiadających dostęp do Rejestru Pełnomocnictw Elektronicznych;
- 3) usunięciu czynności, w stosunku do których jest możliwe udzielenie pełnomocnictwa elektronicznego, o którym mowa w ust. 2 pkt 2.

16. W przypadku usunięcia czynności z informacji, o której mowa w ust. 15, nie jest możliwe wykorzystanie pełnomocnictwa elektronicznego przed danym organem w zakresie tej czynności.

17. Dostęp do Rejestru Pełnomocnictw Elektronicznych zapewnia się:

- 1) podmiotom, o których mowa w art. 2 ust. 1 pkt 1, 2 i 4-8,

2) operatorowi pocztowemu, o którym mowa w art. 3 pkt 12 ustawy z dnia 23 listopada 2012 r. – Prawo pocztowe

– o ile w stosunku do tych podmiotów jest możliwe udzielenie pełnomocnictwa, o którym mowa w ust. 2 pkt 2 i 3.

18. Dostęp, o którym mowa w ust. 17:

- 1) umożliwia pobranie odpisu pełnomocnictwa elektronicznego opatrzonego zaawansowaną pieczęcią elektroniczną ministra właściwego do spraw informatyzacji weryfikowaną przy użyciu kwalifikowanego certyfikatu;
- 2) może nastąpić z wykorzystaniem usługi sieciowej udostępnionej przez ministra właściwego do spraw informatyzacji;
- 3) następuje w zakresie ograniczonym do pełnomocnictw elektronicznych dotyczących czynności realizowanych przez dany podmiot, o którym mowa w ust. 17.

19. Nadanie dostępu, odmowa dostępu oraz cofnięcie dostępu do Rejestru Pełnomocnictw Elektronicznych, o którym mowa w ust. 1, następuje w drodze decyzji administracyjnej.

20. Nadanie dostępu do Rejestru Pełnomocnictw Elektronicznych następuje na wniosek podmiotu zawierający co najmniej:

- 1) nazwę podmiotu składającego wniosek,
- 2) wskazanie, czy w stosunku do tego podmiotu możliwe jest udzielenie pełnomocnictwa elektronicznego, o którym mowa w ust. 2 pkt 2 i 3.

21. Minister właściwy do spraw informatyzacji może umożliwić podmiotowi, o którym mowa w ust. 17 pkt 1, dostęp do Rejestru Pełnomocnictw Elektronicznych za pośrednictwem systemu teleinformatycznego, którego funkcjonowanie zapewnia, o ile podmiot ten realizuje czynności, które mogą być objęte pełnomocnictwem, o którym mowa w ust. 2 pkt 2, bez wydawania decyzji, o której mowa w ust. 19.

22. Minister właściwy do spraw informatyzacji cofa dostęp do Rejestru Pełnomocnictw Elektronicznych:

- 1) na wniosek podmiotu;
- 2) w przypadku braku uzasadnienia dla tego dostępu, w szczególności w przypadku, gdy podmiot zaprzestał realizacji usług lub zadań, o których mowa w art. 20h ust. 2;
- 3) w przypadku gdy minister właściwy do spraw informatyzacji przestał zapewniać techniczną możliwość udzielenia pełnomocnictwa, o którym mowa w ust. 2 pkt 2, w zakresie czynności dotyczących tego podmiotu.

23. Decyzja o cofnięciu dostępu do Rejestru Pełnomocnictw Elektronicznych podlega natychmiastowemu wykonaniu.

24. Każdemu zainteresowanemu, po uwierzytelnieniu oraz po podaniu numeru PESEL mocodawcy oraz numeru pełnomocnictwa elektronicznego, o którym mowa w ust. 2 pkt 4, zapewnia się możliwość:

- 1) weryfikacji istnienia pełnomocnictwa elektronicznego, jego ważności oraz zakresu;
- 2) pobrania z Rejestru Pełnomocnictw Elektronicznych odpisu pełnomocnictwa elektronicznego opatrzonego zaawansowaną pieczęcią elektroniczną ministra właściwego do spraw informatyzacji weryfikowaną przy użyciu kwalifikowanego certyfikatu.

25. Z chwilą udzielenia pełnomocnictwa elektronicznego pełnomocnikowi zapewnia się, w sposób automatyczny, dostęp do udzielonego mu pełnomocnictwa.

26. W Rejestrze Pełnomocnictw Elektronicznych gromadzi się:

- 1) pełnomocnictwa elektroniczne;
- 2) informacje o dacie i godzinie udzielenia pełnomocnictwa elektronicznego;
- 3) informacje o dacie i godzinie odwołania pełnomocnictwa elektronicznego;
- 4) adnotacje, o których mowa w ust. 12 i 13.

27. Minister właściwy do spraw informatyzacji:

- 1) zapewnia ochronę przed nieuprawnionym dostępem do Rejestru Pełnomocnictw Elektronicznych;
- 2) zapewnia integralność danych w Rejestrze Pełnomocnictw Elektronicznych;
- 3) zapewnia dostępność systemu teleinformatycznego, w którym Rejestr Pełnomocnictw Elektronicznych jest prowadzony, dla podmiotów przetwarzających dane w tym rejestrze;
- 4) przeciwdziała uszkodzeniom systemu teleinformatycznego, w którym Rejestr Pełnomocnictw Elektronicznych jest prowadzony;
- 5) określa zasady bezpieczeństwa przetwarzanych danych, w tym danych osobowych;
- 6) zapewnia rozliczalność działań dokonywanych na danych Rejestru Pełnomocnictw Elektronicznych.

28. Danych i zapisów zgromadzonych w Rejestrze Pełnomocnictw Elektronicznych, o którym mowa w ust. 1, nie usuwa się.”.

Art. 4. W ustawie z dnia 6 sierpnia 2010 r. o dowodach osobistych (Dz. U. z 2022 r. poz. 671 oraz z 2023 r. poz. 1234 i 1941) wprowadza się następujące zmiany:

- 1) w art. 66 w ust. 3 po pkt 13b dodaje się pkt 13c w brzmieniu:
„13c) minister właściwy do spraw budownictwa, planowania i zagospodarowania przestrzennego oraz mieszkalnictwa;”;
- 2) w art. 68:
 - a) w ust. 1 uchyla się zdanie drugie,
 - b) po ust. 1 dodaje się ust. 1a i 1b w brzmieniu:
„1a. W przypadku pozytywnej weryfikacji dowodu osobistego w sposób wskazany w ust. 1, wnioskodawca otrzymuje raport o zgodności danych. Raport potwierdza istnienie albo nieistnienie ważnego dowodu osobistego zawierającego określony zestaw danych.
1b. W przypadku negatywnej weryfikacji dowodu osobistego w sposób wskazany w ust. 1, wnioskodawca otrzymuje raport niezgodności wskazujący, która z porównywanych danych została zweryfikowana negatywnie, a w przypadku gdy dokument jest unieważniony – informację o jego unieważnieniu.”,
 - c) dodaje się ust. 7 w brzmieniu:
„7. Udostępnienie fotografii, o którym mowa w art. 68a ust. 1, następuje nieodpłatnie.”;
- 3) po art. 68 dodaje się art. 68a w brzmieniu:
„Art. 68a. 1. Po pozytywnej weryfikacji dowodu osobistego w trybie ograniczonej teletransmisji, z Rejestru Dowodów Osobistych udostępnia się w trybie pełnej teletransmisji fotografię, o której mowa w art. 56 ust. 1 pkt 2.
2. Do korzystania z dostępu do fotografii, o której mowa w art. 56 ust. 1 pkt 2, po wykazaniu konieczności weryfikacji tożsamości klienta w oparciu o fotografię dla podniesienia bezpieczeństwa prowadzonej działalności i uzyskaniu pozytywnej decyzji ministra właściwego do spraw informatyzacji, o której mowa w art. 68 ust. 3, są uprawnieni:
 - 1) przedsiębiorca telekomunikacyjny, będący dostawcą usług, o którym mowa w ustawie z dnia 16 lipca 2014 r. – Prawo telekomunikacyjne (Dz. U. z 2022 r. poz. 1648, 1933 i 2581 oraz z 2023 r. poz. 1394, 1703 i 2005);
 - 2) dostawca usług płatniczych, o którym mowa w art. 4 ust. 2 pkt 4–6 i 12 ustawy z dnia 19 sierpnia 2011 r. o usługach płatniczych (Dz. U. z 2022 r. poz. 2360 i 2640 oraz z 2023 r. poz. 1394 i 1723);
 - 3) podmiot, o którym mowa w art. 4 ust. 1 pkt 1, 17, 18 i 20 ustawy z dnia 29 sierpnia 1997 r. – Prawo bankowe (Dz. U. z 2023 r. poz. 2488);

- 4) spółdzielcza kasa oszczędnościowo-kredytowa lub Krajowa Spółdzielcza Kasa Oszczędnościowo-Kredytowa w rozumieniu ustawy z dnia 5 listopada 2009 r. o spółdzielczych kasach oszczędnościowo-kredytowych (Dz. U. z 2023 r. poz. 1278, 1394, 1407, 1723 i 1843);
- 5) kwalifikowany dostawca usług zaufania, wpisany do rejestru dostawców usług zaufania, o którym mowa w art. 2 pkt 1 ustawy z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej (Dz. U. z 2021 r. poz. 1797 oraz z 2023 r. poz. 1234);
- 6) podmiot, o którym mowa w art. 59d ustawy z dnia 12 maja 2011 r. o kredycie konsumenckim (Dz. U. z 2023 r. poz. 1028, 1285, 1394 i 1723);
- 7) podmiot wydający środki identyfikacji elektronicznej w systemie identyfikacji elektronicznej zgodnie z ustawą z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej.

3. W celu potwierdzenia tożsamości osoby wnioskującej o potwierdzenie profilu zaufanego podmiotom, o których mowa w art. 20c ust. 2, 3 i 8 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne może zostać udostępniona fotografia, o której mowa w art. 56 ust. 1 pkt 2.

4. Podmiotom, o których mowa w art. 20c ust. 8 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne, może zostać udostępniona fotografia, o której mowa w art. 56 ust. 1 pkt 2, po spełnieniu warunków określonych w ust. 2.

5. Udostępnieniu w trybie, o którym mowa w ust. 1, podlega fotografia zamieszczona w ostatnim wydanym dowodzie osobistym, który w dniu dokonywania jego weryfikacji w trybie ograniczonej teletransmisji jest dokumentem ważnym.”.

Art. 5. W ustawie z dnia 24 września 2010 r. o ewidencji ludności (Dz. U. z 2022 r. poz. 1191 oraz z 2023 r. poz. 497, 1394 i 1941) wprowadza się następujące zmiany:

- 1) w art. 23e w ust. 2 w pkt 1 lit. b otrzymuje brzmienie:
„b) przy użyciu certyfikatu podstawowego, o którym mowa w art. 2 pkt 2 ustawy z dnia 26 maja 2023 r. o aplikacji mObywatel (Dz. U. poz. 1234);”;
- 2) w art. 23j w ust. 2 w pkt 1 lit. b otrzymuje brzmienie:
„b) przy użyciu certyfikatu podstawowego, o którym mowa w art. 2 pkt 2 ustawy z dnia 26 maja 2023 r. o aplikacji mObywatel, oraz”.

Art. 6. W ustawie z dnia 23 listopada 2012 r. – Prawo pocztowe (Dz. U. z 2023 r. poz. 1640) w art. 38:

1) ust. 2 otrzymuje brzmienie:

„2. Pełnomocnictwo pocztowe obejmuje:

- 1) imię i nazwisko oraz numer PESEL osoby udzielającej pełnomocnictwa;
- 2) zakres pełnomocnictwa;
- 3) imię i nazwisko oraz numer PESEL pełnomocnika.”;

2) ust. 3a otrzymuje brzmienie:

„3a. Pełnomocnictwa pocztowego adresat może również udzielić przez złożenie w postaci elektronicznej oświadczenia opatrzonego:

- 1) kwalifikowanym podpisem elektronicznym,
- 2) podpisem zaufanym,
- 3) podpisem osobistym albo
- 4) zaawansowaną pieczęcią elektroniczną ministra właściwego do spraw informatyzacji, po uwierzytelnieniu wnioskodawcy przy użyciu certyfikatu podstawowego, o którym mowa w art. 2 pkt 2 ustawy z dnia 26 maja 2023 r. o aplikacji mObywatel (Dz. U. poz. 1234 i ...)

– jeżeli operator pocztowy przewidział taką możliwość w regulaminie świadczenia usług pocztowych lub regulaminie świadczenia usług powszechnych.”.

Art. 7. W ustawie z dnia 18 listopada 2020 r. o doręczeniach elektronicznych (Dz. U. z 2023 r. poz. 285 i 1860) wprowadza się następujące zmiany:

1) w art. 152:

a) w ust. 1 we wprowadzeniu do wyliczenia wyrazy „po dniu 31 grudnia 2023 r.” zastępuje się wyrazami „od dnia 1 stycznia 2025 r.”,

b) w ust. 2 wprowadzenie do wyliczenia otrzymuje brzmienie:

„Podmioty niepubliczne nieposiadające adresu do doręczeń elektronicznych wpisanego do bazy adresów elektronicznych, wpisane do Centralnej Ewidencji i Informacji o Działalności Gospodarczej do dnia 31 grudnia 2024 r., składające w okresie od dnia 1 lipca 2025 r. do dnia 30 września 2026 r. wniosek o zmianę wpisu, są obowiązane do:”;

2) w art. 155 w ust. 11 wyrazy „1 stycznia 2024 r.” zastępuje się wyrazami „1 stycznia 2025 r.”.

Art. 8. W ustawie z dnia 26 maja 2023 r. o aplikacji mObywatel (Dz. U. poz. 1234) wprowadza się następujące zmiany:

- 1) w art. 3 w ust. 1 w pkt 7 kropkę zastępuje się średnikiem i dodaje się pkt 8 w brzmieniu:
„8) korzystanie z usług online, udostępnionych na zasadach określonych w art. 19aa ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne.”;
- 2) w art. 14 po ust. 5 dodaje się ust. 5a i 5b w brzmieniu:
„5a. Dane lub dokumenty związane z potwierdzeniem tożsamości użytkownika aplikacji mObywatel w sposób, o którym mowa w art. 4 ust. 1, które posiadają postać elektroniczną, są przechowywane i archiwizowane w systemie mObywatel.
5b. Jeżeli z przepisów prawa wynika obowiązek udostępnienia danych lub dokumentów, posiadających postać elektroniczną, związanych z potwierdzeniem tożsamości użytkownika aplikacji mObywatel w sposób, o którym mowa w art. 4 ust. 1, minister właściwy do spraw informatyzacji rozpatruje wnioski o takie udostępnienie oraz w uzasadnionych przypadkach dokonuje udostępnienia takich danych oraz dokumentów.”;
- 3) w art. 19 w ust. 1 w pkt 7:
 - a) lit. a otrzymuje brzmienie:
„a) usługę w aplikacji mObywatel,”;
 - b) w lit. b średnik zastępuje się przecinkiem i dodaje się lit. c w brzmieniu:
„c) usługę online dla dokumentów mobilnych, biorąc pod uwagę potrzeby weryfikujących i użytkowników aplikacji mObywatel;”.

Art. 9. 1. Podmioty, o których mowa w art. 68a ust. 2 i 4 ustawy zmienianej w art. 4, w dniu określonym w komunikacie, o którym mowa w art. 13, posiadające decyzję, o której mowa w art. 68 ust. 3 ustawy zmienianej w art. 4, mogą wystąpić do ministra właściwego do spraw informatyzacji o wyrażenie zgody na udostępnianie fotografii z Rejestru Dowodów Osobistych w trybie teletransmisji, po wykazaniu konieczności weryfikacji tożsamości klienta w oparciu o fotografię, dla podniesienia bezpieczeństwa prowadzonej działalności.

2. Wyrażenie zgody, o której mowa w ust. 1, następuje przez zmianę decyzji, o której mowa w art. 68 ust. 3 ustawy zmienianej w art. 4.

Art. 10. Dotychczasowe przepisy wykonawcze wydane na podstawie art. 197 pkt 1-5 ustawy zmienianej w art. 2 zachowują moc do dnia wejścia w życie przepisów wykonawczych

wydanym na podstawie art. 197 ust. 1-5 ustawy zmienianej w art. 2, w brzmieniu nadanym niniejszą ustawą, jednak nie dłużej niż do dnia 12 lipca 2024 r. i mogą być zmieniane.

Art. 11. Minister właściwy do spraw informatyzacji ogłasza w Dzienniku Urzędowym Rzeczypospolitej Polskiej „Monitor Polski” komunikat określający dzień i zakres wdrożenia rozwiązań technicznych, o których mowa w art. 3 pkt 4 w zakresie art. 19ab ust. 1 pkt 3 i art. 19ac.

2. Komunikat, o którym mowa w ust. 1, ogłasza się w terminie co najmniej 14 dni przed dniem wdrożenia rozwiązań technicznych, określonym w tym komunikacie.

Art. 12. Minister właściwy do spraw informatyzacji ogłasza w Dzienniku Urzędowym Rzeczypospolitej Polskiej „Monitor Polski” komunikat określający dzień i zakres wdrożenia rozwiązań technicznych, o których mowa w art. 2 pkt 2.

2. Komunikat, o którym mowa w ust. 1, ogłasza się w terminie co najmniej 14 dni przed dniem wdrożenia rozwiązań technicznych, określonym w tym komunikacie.

Art. 13. Minister właściwy do spraw informatyzacji ogłasza w Dzienniku Urzędowym Rzeczypospolitej Polskiej „Monitor Polski” komunikat określający dzień i zakres wdrożenia rozwiązań technicznych, o których mowa w art. 4 pkt 2 i 3.

2. Komunikat, o którym mowa w ust. 1, ogłasza się w terminie co najmniej 14 dni przed dniem wdrożenia rozwiązań technicznych, określonym w tym komunikacie.

Art. 14. Ustawa wchodzi w życie po upływie 14 dni od dnia ogłoszenia, z wyjątkiem:

- 1) art. 1 i art. 3 pkt 4 w zakresie art. 19ab ust. 1 pkt 3 i art. 19ac, które w które wychodzą w życie z dniem określonym w komunikacie, o którym mowa w art. 11;
- 2) art. 2 pkt 2, który wchodzi w życie z dniem określonym w komunikacie, o którym mowa w art. 12;
- 3) art. 3 pkt 2, który wchodzi w życie z dniem 1 stycznia 2025 r.;
- 4) art. 4 pkt 2 i 3, które wchodzi w życie z dniem określonym w komunikacie, o którym mowa w art. 13;
- 5) art. 7, który wchodzi w życie z dniem następującym po dniu ogłoszenia.

UZASADNIENIE

Wprowadzenie

Celem projektowanej ustawy jest wprowadzenie podstaw prawnych dla funkcjonowania rozwiązań usprawniających oraz rozwijających funkcjonowanie e-administracji, w zakresie dostarczania obywatelom usług cyfrowych. Intensywny proces transformacji cyfrowej polskiej administracji wymaga dostosowania otoczenia prawnego do dynamicznie zmieniającej się rzeczywistości. W 2008 r. została wdrożona platforma ePUAP i istnieje potrzeba jej ciągłej modernizacji, jak również innych systemów służących do zapewniania nowoczesnych e-usług obywatelom. Zaproponowane rozwiązania pozwolą zintensyfikować rozwój usług wprowadzając nowy dokument strategiczny oraz nowe podstawy prawne udostępniania e-usług.

Ustawy zmieniane w projekcie

Niniejszą ustawą zmienia się ustawy: ustawę z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego, ustawę z dnia 21 sierpnia 1997 r. o gospodarce nieruchomościami, ustawę z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne, ustawę z dnia 6 sierpnia 2010 r. o dowodach osobistych, ustawę z dnia 24 września 2010 r. o ewidencji ludności, ustawę z dnia 23 listopada 2012 r. – Prawo pocztowe, ustawę z dnia 18 listopada 2020 r. o doręczeniach elektronicznych oraz ustawę z dnia 26 maja 2023 r. o aplikacji mObywatel.

Ustawa z dnia 21 sierpnia 1997 r. o gospodarce nieruchomościami oraz ustawa z dnia 6 sierpnia 2010 r. o dowodach osobistych

Dotychczasowe świadectwo uprawnień rzeczoznawcy majątkowego może być wydawane według obecnie obowiązującego wzoru nie dłużej niż 5 lat do dnia wejścia w życie ustawy z dnia 22 listopada 2018 r. o dokumentach publicznych, czyli maksymalnie do dnia 11 lipca 2024 r. (art. 73 ust. 1 pkt 2 ustawy z dnia 22 listopada 2018 r. o dokumentach publicznych). W związku z powyższym zdecydowano, że nowe świadectwo powinno mieć formę dwustronnej spersonalizowanej karty identyfikacyjnej. Jednocześnie, mając na uwadze postępujący rozwój cyfryzacji wszelkiego rodzaju usług, w ramach modyfikacji wzoru świadectwa przewidziano również możliwość wydania tego dokumentu, w postaci dokumentu mobilnego obsługiwanego przy użyciu usługi udostępnianej w aplikacji mobilnej mObywatel. Opracowanie nowego wzoru świadectwa oraz umożliwienie udostępnienia tego dokumentu w aplikacji mObywatel wymaga jednak stworzenia na gruncie ustawowym podstaw prawnych do tego rodzaju działań.

W tym celu zaproponowano zmianę art. 192 ustawy z dnia 21 sierpnia 1997 r. o gospodarce nieruchomościami regulującego kwestie wydawania świadectw nadania uprawnień zawodowych w zakresie szacowania nieruchomości.

Ponadto uwzględniając fakt, że jednym z elementów świadectwa nadania uprawnień jest fotografia rzeczoznawcy majątkowego i równocześnie mając na względzie, że w wersji elektronicznej świadectwa w aplikacji mObywatel zawarta będzie fotografia pobrana z Rejestru Dowodów Osobistych (RDO), zaproponowano, aby analogiczne zdjęcie zamieszczane było również na wersji fizycznej świadectwa. Zaproponowane rozwiązanie będzie korzystne dla rzeczoznawców majątkowych, bowiem wyeliminuje koszty związane z potrzebą zrobienia oddzielnej fotografii, a zarazem dokument „fizyczny” będzie jednorodny wizualnie z jego postacią mobilną. Proponowany sposób pozyskiwania fotografii koresponduje przy tym z tendencją pozyskiwania danych, które są dostępne w jednym rejestrze publicznym na potrzeby innego systemu bezpośrednio z tego rejestru, tak aby obywatel nie musiał przekazywać kilka razy tych samych informacji danych organom administracji (tzw. zasada jednego źródła danych).

Zaproponowano rozszerzenie delegacji ustawowej sformułowanej w art. 197 ustawy z dnia 21 sierpnia 1997 r. o gospodarce nieruchomościami, w zakresie pkt 3, umożliwiając określenie w drodze rozporządzenia wzorów dokumentów związanych z nadaniem uprawnień zawodowych w zakresie szacowania nieruchomości, w szczególności świadectwa nadania tych uprawnień, a także warunków i trybu wydawania tych dokumentów. Ta zmiana wymaga dodatkowo wprowadzenia przepisu przejściowego rozstrzygającego o zachowaniu w mocy dotychczasowego aktu wykonawczego wydawanego na podstawie ww. przepisu.

Wdrożenie nowego wzoru świadectwa nadania uprawnień zawodowych, w tym także pobierania fotografii rzeczoznawcy majątkowego z RDO oraz udostępniania tego dokumentu w aplikacji mObywatel powinno nastąpić z dniem 12 lipca 2024 r., czyli, tak jak wskazano powyżej, od dnia następującego po dniu, do którego możliwe jest wydawanie dokumentów publicznych trzeciej kategorii w obecnej formie.

Ustawa z dnia 6 sierpnia 2010 r. o dowodach osobistych – udostępnianie wizerunku w celu przeciwdziałania kradzieży tożsamości

W ustawie z dnia 6 sierpnia 2010 r. o dowodach osobistych proponuje się wprowadzenie zmian, których głównym celem jest podniesienie skuteczności oraz bezpieczeństwa procesów ustalania tożsamości osób fizycznych przez zapewnienie warunków pozwalających na

uzupełnienia tych procesów o weryfikację wizerunku twarzy osoby fizycznej z wizerunkiem tej osoby przechowywanym w Rejestrze Dowodów Osobistych (RDO).

Konsultacje przeprowadzone w ramach procesu legislacyjnego projektu ustawy o zmianie niektórych ustaw w związku z rozwojem e-administracji (UD372) z dostawcami usług świadczonych w sektorze prywatnym prowadzą do konkluzji, że zapewnienie dostępu do danej biometrycznej, jaką stanowi wizerunek osoby fizycznej przechowywany w RDO, wpłynie pozytywnie na uszczelnienie procedur ustalania tożsamości osób fizycznych, co w rezultacie przełoży się na znaczne ograniczenie liczby wyłudzeń, które mają miejsce szczególnie w sektorze finansowym. Zgodnie z ustaleniami proceder tzw. „kradzieży tożsamości” realizowany jest głównie z wykorzystaniem imitacji dowodów osobistych. W takich przypadkach sfałszowany dokument zawiera zdjęcie sprawcy oraz dane ofiary, pod którą podszywa się sprawca. Wobec powyższego sama weryfikacja danych zawartych w okazywanym dowodzie osobistym, a w niektórych przypadkach także zabezpieczeń fizycznych takiego dokumentu, może prowadzić usługodawcę do fałszywego przekonania o prawdziwości okazywanego dokumentu. Zapewnienie usługodawcom możliwości weryfikacji, oprócz danych jakie zawiera dowód osobisty, także zdjęcia jakie zawiera autentyczny dokument, znacząco wpłynie na ukrócenie wyżej opisanego procederu.

W projekcie proponuje się przyjęcie dwustopniowego modelu dostępu usługodawcy do wizerunku twarzy. Zgodnie z przyjętymi założeniami, w pierwszym kroku usługodawca będzie musiał uzyskać pozytywny wynik weryfikacji danych zawartych w weryfikowanym dowodzie osobistym. Weryfikacja ta będzie odbywała się przy użyciu usługi sieciowej, udostępnianej przez ministra właściwego do spraw informatyzacji, która funkcjonuje już obecnie na podstawie aktualnych przepisów zmienianej ustawy. Usługodawca ubiegający się o dostęp do wizerunku twarzy będzie musiał uprzednio uzyskać pozytywną decyzję ministra właściwego do spraw informatyzacji warunkującą uzyskanie dostępu do danych zgromadzonych w RDO, w trybie weryfikacji danych, za pośrednictwem ww. usługi sieciowej. Dopiero po potwierdzeniu istnienia dowodu osobistego w wyżej opisany sposób, usługodawca będzie miał zapewnioną możliwość weryfikacji fotografii posiadacza dowodu osobistego, przechowywanej w RDO, przy użyciu usługi sieciowej udostępnionej przez ministra właściwego do spraw informatyzacji, w trybie pełnej teletransmisji.

Katalog podmiotów, którym zapewniony zostanie dostęp do wizerunku twarzy, określono przez pryzmat wykonywanych zadań i czynności, w których niezbędna jest skuteczna weryfikacja tożsamości klienta. Jednocześnie, niezależnie od zakresu wykonywanych zadań,

podmiot ubiegający się o dostęp do wizerunku twarzy będzie musiał wykazać konieczność weryfikacji tożsamości klienta w oparciu o fotografię. Tym samym posiadanie przez usługodawcę wyłącznie dostępu do danych zgromadzonych w RDO w drodze weryfikacji nie będzie stanowiło automatycznej przepustki do dostępu do wizerunku posiadacza dowodu osobistego.

W ramach dalszych zmian w art. 68 ustawy dnia 6 sierpnia 2010 r. o dowodach osobistych, proponuje się dodanie ust. 1b dotyczącego udostępniania, w przypadku negatywnej weryfikacji dowodu osobistego, raportu niezgodności danych. Raport niezgodności danych ma zapewnić sprawną obsługę klienta przez podmiot komercyjny np. bank oraz ją przyspieszyć, a także ograniczyć konieczność wizyty klienta banku w urzędzie w celu weryfikacji zapisu danych osoby widniejącej w wydany jej dowodzie osobistym. Obecnie, jak również sygnalizuje Związek Banków Polskich, proces weryfikacji pomimo posługiwania się przez klienta ważnym dokumentem sprawia trudności i odbija się negatywnie na kliencie, w szczególności w przypadku występowania w danych osoby znaków diakrytycznych. Brak informacji, że negatywna weryfikacja spowodowana jest wadliwym wskazaniem określonej kategorii danych często powoduje odesłanie klienta do urzędu w celu wyjaśnienia sprawy i weryfikacji zapisów danych osoby widniejącej w rejestrze państwowym. Niejednokrotnie są to również zwykłe omyłki i literówki podczas wpisywania danych, które również powodują odesłanie klienta do urzędu. Problem ten jest obserwowany również z poziomu urzędu obsługującego ministra właściwego do spraw informatyzacji, który w odpowiedzi na indywidualne zapytania osób fizycznych kierowane do niej bezpośrednio sprawdza sposób wprowadzenia zapytania przez podmioty weryfikujące. Sytuacje te dotyczą często spraw ważnych z punktu widzenia np. prowadzonej działalności gospodarczej i dokonywanych w jej ramach operacji finansowych, gdzie istotny jest czas obsługi zlecenia.

Rozszerzenie raportu weryfikacji o wskazanie, która z danych jest niezgodna, mieści się zatem w realizacji celu w jakim każdorazowo podmiot wnioskuje o weryfikację, jak również znajduje się w ramach celu, któremu służy ten tryb udostępniania. Tryb weryfikacji (ograniczonej teletransmisji) polega przede wszystkim na ustaleniu, czy dowód osobisty o wskazanym zakresie danych istnieje, czy też nie. Nie ma jednak przeszkód, aby podmiot weryfikujący, który co należy podkreślić, na mocy decyzji wydanej przez ministra właściwego do spraw informatyzacji, jest do tego uprawniony, uzyskał również informację, która konkretnie dana jest niezgodna. Nadal nie jest to bowiem udostępnienie tej danej, a jedynie wskazanie, która z nich jest nieprawidłowa. W dalszym ciągu podmiot taki po uzyskaniu

raportu niezgodności powinien podchodzić ostrożnie co do legalności tak zweryfikowanego dowodu osobistego. Celem nowelizacji jest przede wszystkim wsparcie podmiotów sektora prywatnego w prowadzonej przez nie działalności, tak aby podmioty te mogły wywiązywać się z ustawowo nałożonych na nie obowiązków, w tym weryfikować dane swoich klientów. Uzyskanie takiego raportu daje im dodatkowo możliwość zweryfikowania po swojej stronie, czy aby wszystkie dane zostały wpisane poprawnie i czy nie należy ich ponownie uzupełnić i zweryfikować, bez narażania klienta na niepotrzebne nieprzyjemności.

Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne

W projekcie przewidziano wprowadzenie upoważnienia ustawowego dla ministra właściwego do spraw informatyzacji do opracowania dokumentu strategicznego, którego celem będzie określenie kierunków procesu informatyzacji państwa, mając na uwadze:

- potrzebę przygotowania kompleksowego i długoterminowego dokumentu o charakterze strategicznym, który zapewniłby wieloletnią perspektywę rozwoju procesu informatyzacji państwa,
- efektywność i celowość wydatkowania środków z budżetu państwa oraz funduszy europejskich na działania w obszarze cyfryzacji.

Strategia uwzględni dotychczas zrealizowane działania oraz poziom zastosowania nowoczesnych technologii w administracji publicznej na rzecz obywateli, weźmie pod uwagę założenia komplementarnych dokumentów strategicznych i programowych rządu w tym obszarze. Strategia zastąpi Program Zintegrowanej Informatyzacji Państwa, a zakresem przedmiotowym obejmie działania będące w zakresie kompetencji Rady Ministrów. Dokument będzie miał charakter strategiczny, natomiast nie będzie stanowił strategii rozwoju w rozumieniu ustawy z dnia 6 grudnia 2006 r. o zasadach prowadzenia polityki rozwoju. Dokument ten będzie przyjmowany na mocy ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (podobnie jak w przypadku przyjęcia strategii cyberbezpieczeństwa na mocy ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa). Dokument, o którym mowa, będzie obejmował okres wykraczający poza dotychczas przyjęte strategie rozwoju, co jest konieczne z uwagi na potrzebę dobrego planowania, spójności i ciągłości procesów cyfrowych państwa, które z uwagi na wieloletnią perspektywę budowania Architektury Informacyjnej Państwa wymagają koordynacji ministra właściwego do spraw informatyzacji. W proces przygotowania i realizacji założeń strategii

zaangażowane zostaną pozostałe ministerstwa, w celu zapewnienia harmonizacji i komplementarności realizowanych i planowanych działań na rzecz interesariuszy procesu informatyzacji państwa, w tym administracji publicznej. Strategia będzie również stanowiła podstawę do określenia sposobów i zasad współpracy wewnątrz administracji rządowej oraz z pozostałymi interesariuszami cyfryzacji państwa, w tym jednostkami samorządu terytorialnego.

Zmiany dotyczą również uprawnienia ministra właściwego do spraw informatyzacji do udostępniania usług online oraz zbiorczych usług online przy wykorzystaniu systemów teleinformatycznych ministra oraz publicznej aplikacji mobilnej, w celu wykonywania zadań publicznych zarówno przez ministra jak też przez inne podmioty publiczne. W skład tych usług wchodzi zarządzanie skrzynką doręczeń, w rozumieniu z dnia 18 listopada 2020 r. o doręczeniach elektronicznych, dostępem do konta ePUAP oraz udzielaniem i dostępem do pełnomocnictw gromadzonych w Rejestrze Pełnomocnictw Elektronicznych. Zgodnie z projektowanymi przepisami usługi online mogą być dostosowane do potrzeb użytkownika na podstawie jego danych, a szczególnie danych osobowych użytkownika oraz danych dotyczących sytuacji prawnej tego użytkownika lub praw mu przysługujących, umożliwiających identyfikację rzeczy związanej z tym użytkownikiem pobranych z rejestrów publicznych lub systemów teleinformatycznych podmiotów publicznych. Nowelizacja obejmuje przyznanie ministrowi właściwemu do spraw informatyzacji uprawnienia do otrzymywania danych niezbędnych do udostępniania usług online w tym danych osobowych użytkownika oraz danych dotyczących jego sytuacji prawnej lub praw mu przysługujących oraz danych dotyczące wierzytelności. Proponowane przepisy określają warunki uwierzytelnienia użytkownika jakie są wymagane w celu korzystania z usług online oraz cechy systemu teleinformatycznego wykorzystywanego do udostępniania usług online. Wprowadzona została również możliwość zawierania przez ministra właściwego do spraw informatyzacji porozumień z podmiotami publicznymi określających sposób, zakres i tryb udostępniania danych i usług online. Zakres przekazywanych danych wynika z rodzaju usługi jaka będzie udostępniana, a zatem nie jest możliwe precyzyjne wskazanie o jakie konkretnie przekazywane dane osobowe chodzi, gdyż w zależności od udostępnianej usługi będą one ulegały zmianie. Dane te przekazywane są w trybie wymiany informacji między systemami teleinformatycznymi ministra właściwego do spraw informatyzacji a systemem teleinformatycznym podmiotu, na rzecz którego realizowana jest ta usługa, w zakresie niezbędnym do jej realizacji i nie zachodzi potrzeba wskazywania technicznych aspektów ich przekazywania w normach prawnych. Z

uwagi na fakt, iż udostępnianie ogólnych warunków jest fakultatywne, w opinii projektodawcy nie zachodzi potrzeba wskazywania trybu ich określania.

Celem nowelizacji jest również umocowanie Rejestru Pełnomocnictw Elektronicznych, którego przeznaczeniem jest gromadzenie informacji o pełnomocnictwach udzielanych między osobami fizycznymi posiadającymi numer PESEL. W zakresie pełnomocnictw elektronicznych rejestr ten będzie rejestrem referencyjnym dla innych systemów administracji publicznej. Wprowadzenie rejestru sankcjonuje również możliwość posługiwania się odpisem danych o pełnomocnictwie elektronicznym, przechowywanym w ramach tego rejestru. Rejestr będzie udostępniał usługę weryfikacji danych o pełnomocnictwie elektronicznym. Z punktu widzenia obywatela, wprowadzany rejestr pozwoli na zarządzanie wszystkimi pełnomocnictwami elektronicznymi z poziomu jednego punktu dostępu oraz zagwarantuje mu pewność honorowania takiego pełnomocnictwa, jeśli taka możliwość będzie prawnie przewidziana. Minister właściwy do spraw informatyzacji na wniosek operatora pocztowego zapewni również możliwość udzielania elektronicznych pełnomocnictw pocztowych. Treść pełnomocnictwa ustalana będzie zgodnie z art. 38 ust. 2 ustawy z dnia 23 listopada 2012 r. – Prawo pocztowe. Do uwierzytelniania pełnomocnictwa pocztowego stosuje się ustawę z dnia 23 listopada 2012 r. – Prawo pocztowe.

Zaproponowana regulacja w zakresie pełnomocnictw elektronicznych nie obejmuje swoim zasięgiem kwestii dotyczących pełnomocnictw w prawie podatkowym. Prawo podatkowe posiada bowiem odrębne uregulowania, tj. w ustawie z dnia 29 sierpnia 1997 r. – Ordynacja podatkowa zostały określone rodzaje i forma, sposób składania oraz rejestr pełnomocnictw etc.

Wprowadzone w zakresie pełnomocnictw elektronicznych zmiany nie modyfikują ani nie wpływają na formę udzielenia i odwołania pełnomocnictwa, rodzaj oraz zakresu stosowania przepisów Kodeksu cywilnego do pełnomocnictw elektronicznych, bowiem to te przepisy określają, kiedy, jakiego rodzaju oraz w jakiej formie może być udzielone oraz odwołane pełnomocnictwo. Pełnomocnictwo elektroniczne może być zastosowane tylko wówczas, gdy przepisy Kodeksu cywilnego umożliwiają zastosowanie takiego pełnomocnictwa w takiej formie, a odwołanie tego pełnomocnictwa będzie możliwe w przypadku i na zasadach określonych w Kodeksie cywilnym.

Ustawa z dnia 24 września 2010 r. o ewidencji ludności

Zmiany zaproponowane w ustawie z dnia 24 września 2010 r. o ewidencji ludności (Dz. U. z 2022 r. poz. 1191 oraz z 2023 r. poz. 497, 1394 i 1941) mają na celu ich dostosowanie do obowiązujących przepisów dotyczących używania certyfikatów określonych w ustawie z dnia 26 maja 2023 r. o aplikacji mObywatel (Dz. U. poz. 1234).

Ustawa z dnia 23 listopada 2012 r. - Prawo pocztowe

W ustawie z dnia 23 listopada 2012 r. – Prawo pocztowe wprowadzono zmiany dotyczące możliwości udzielania elektronicznych pełnomocnictw pocztowych. Zagadnienie zostało szerzej opisane w akapicie dotyczącym zmian w ustawie z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne.

Ustawa z dnia 18 listopada 2020 r. o doręczeniach elektronicznych

Na podstawie art. 155 ust. 10 ustawy z dnia 18 listopada 2020 r. o doręczeniach elektronicznych w dniu 29 maja 2023 r. został ogłoszony komunikat Ministra Cyfryzacji w sprawie określenia terminu wdrożenia rozwiązań technicznych niezbędnych do doręczania korespondencji z wykorzystaniem publicznej usługi rejestrowanego doręczenia elektronicznego lub publicznej usługi hybrydowej oraz udostępnienia w systemie teleinformatycznym punktu dostępu do usług rejestrowanego doręczenia elektronicznego w ruchu transgranicznym (Dz. U. poz. 1077) wskazujący termin wejścia w życie obowiązku stosowania doręczeń elektronicznych przez podmioty wskazane w ustawie o doręczeniach elektronicznych. Dzień ten został wskazany na 10 grudnia 2023 r. Dnia 23 listopada 2023 r. został ogłoszony komunikat Ministra Cyfryzacji z dnia 22 listopada 2023 r. zmieniający komunikat w sprawie określenia terminu wdrożenia rozwiązań technicznych niezbędnych do doręczania korespondencji z wykorzystaniem publicznej usługi rejestrowanego doręczenia elektronicznego lub publicznej usługi hybrydowej oraz udostępnienia w systemie teleinformatycznym punktu dostępu do usług rejestrowanego doręczenia elektronicznego w ruchu transgranicznym (Dz. U. poz. 2540), w którym nowy termin ustalono na 30 grudnia 2023 r.

Zgodnie z art. 155 ust. 11 ustawy z dnia 18 listopada 2020 r. o doręczeniach elektronicznych termin ten nie może być późniejszy niż 1 stycznia 2024 r.

W ostatnim czasie do urzędu obsługującego ministra właściwego do spraw informatyzacji spłynęło wiele wniosków od organizacji zrzeszających podmioty publiczne, zawody zaufania publicznego oraz innych, na które ustawa nakłada obowiązek podłączenia do systemu e-doręczeń dotyczących konieczności przesunięcia terminu wdrożenia obowiązku stosowania

doręczeń elektronicznych, gdyż czas na wdrożenie nowego rozwiązania w zakresie prowadzenia korespondencji okazał się niewystarczający dla podmiotów.

Samorządowcy zwrócili również uwagę na to, że termin wejścia w życie obowiązku korzystania z doręczeń elektronicznych przypada tuż przed dużą wysyłką realizowaną w jednostkach samorządu terytorialnego – tj. obowiązkiem wysłania, w pierwszych tygodniach każdego roku, decyzji ustalających wymiar podatku od nieruchomości. Jest to duże przedsięwzięcie organizacyjne w gminach, które wysyłają w tym okresie 50% korespondencji wysyłanej przez cały rok.

Wdrożenie doręczeń elektronicznych wymaga więcej czasu. Oprócz integracji pod względem technicznym (zintegrowanie doręczeń elektronicznych z systemem kancelaryjnym) należy wprowadzić zmiany organizacyjne, w tym dokonać przeglądu wewnętrznych procedur w zakresie prowadzenia korespondencji, przeanalizować przepisy, przeszkolić pracowników.

W odpowiedzi na postulaty środowisk zrzeszających podmioty zobowiązane do stosowania doręczeń elektronicznych została podjęta decyzja o przesunięciu terminu wejścia w życie obowiązku stosowania doręczeń elektronicznych na termin późniejszy, jednak nie później niż 1 stycznia 2025 r. Dokładny termin zostanie wskazany w komunikacie, który zostanie wydany co najmniej 90 dni przed tym terminem.

Dodatkowo minister właściwy do spraw informatyzacji planuje również wdrożenie we współpracy z operatorem wyznaczonym funkcjonalności i zmian w systemie, które zapewnią sprawniejszą obsługę korespondencji, szczególnie w podmiotach publicznych, w tym: funkcjonalność pozwalającą na masowe wysyłanie wiadomości do wielu adresatów, masową archiwizację wiadomości w skrzynce doręczeń czy zwiększenie możliwości do wysyłania wielkości załączników za pośrednictwem publicznej usługi rejestrowanego doręczenia elektronicznego.

Celem ministra właściwego do spraw informatyzacji jest zapewnienie bezpiecznej i w pełni elektronicznej, rejestrowanej korespondencji w administracji publicznej, a docelowo w całej gospodarce. Dlatego też dąży się do zapewnienia powszechnego wykorzystania doręczeń elektronicznych jako usługi bezpiecznej i zgodnej z europejskim rozporządzeniem Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylającego dyrektywę 1999/93/WE. Wdrożenie nowego rozwiązania na tak dużą skalę – wszystkie podmioty publicznej, zawody zaufania publicznego, przedsiębiorcy

wpisani do CEIDG oraz podmioty wpisane do KRS – jest procesem, który musi następować stopniowo i odbywać się równolegle z działaniami informacyjnymi (tj. upowszechnienie podstawowej wiedzy nt. nowego rozwiązania) oraz działaniami promocyjnymi (przedstawienie korzyści z nowego rozwiązania).

Ustawa z dnia 26 maja 2023 r. o aplikacji mObywatel

Zmiana ma na celu doprecyzowanie organu odpowiedzialnego, za przechowywanie i archiwizację danych lub dokumentów związanych z procesami potwierdzania tożsamości użytkowników aplikacji mObywatel, o których mowa w art. 4 ust. 1 ustawy z dnia 26 maja 2023 r. o aplikacji mObywatel. Dostarczenie, w ramach systemu mObywatel, rozwiązania umożliwiającego potwierdzanie tożsamości zapewni minister właściwy do spraw informatyzacji. Dlatego przechowywanie danych lub dokumentów elektronicznych wytworzonych w trakcie tego procesu, powinno odbywać się tylko po stronie systemu mObywatel. Aby ograniczyć obowiązki organów gminy związane z przechowywaniem danych i dokumentów elektronicznych, proces ten w całości obsłuży minister właściwy do spraw informatyzacji.

Ponadto zasadnie jest, aby uregulować procedurę uzyskania danych lub dokumentów elektronicznych przechowywanych i archiwizowanych przez ministra właściwego do spraw informatyzacji przez osoby wnioskujące, tak aby zapewnić bezpieczeństwo tych danych.

W celu zwiększenia dostępności usług umożliwiających przeprowadzenie weryfikacji kryptograficznej, o której mowa w art. 19 ust. 1 pkt 7 ustawy z dnia 26 maja 2023 r. o aplikacji mObywatel, uzasadnione jest rozszerzenie zbioru narzędzi do weryfikacji o usługę online, tj. weryfikator w wersji webowej. Nowa usługa online będzie umożliwiała w pierwszej kolejności przeprowadzenie weryfikacji kryptograficznej dokumentu mObywatel (funkcjonującego pod biznesową nazwą „mDowód”). W tym modelu osoba weryfikująca nie będzie potrzebowała telefonu. Z uwagi na charakter tej usługi online uzasadnione jest, aby weryfikacja kolejnych dokumentów mobilnych, w ramach takiej usługi online, była dostarczana sukcesywnie w zależności od potrzeb zgłaszanych przez weryfikujących oraz użytkowników aplikacji mObywatel.

Przepisy o wejściu w życie

Ustawa wchodzi w życie po upływie 14 dni od dnia ogłoszenia, z wyjątkiem:

- 1) art. 1 i art. 3 pkt 4 w zakresie art. 19ab ust. 1 pkt 3 i art. 19ac, które w które wychodzą w życie z dniem określonym w komunikacie, o którym mowa w art. 11;

- 2) art. 2 pkt 2, który wchodzi w życie z dniem określonym w komunikacie, o którym mowa w art. 12;
- 3) art. 3 pkt 2, który wchodzi w życie z dniem 1 stycznia 2025 r.;
- 4) art. 4 pkt 2 i 3, które wchodzi w życie z dniem określonym w komunikacie, o którym mowa w art. 13;
- 5) art. 7, który wchodzi w życie z dniem następującym po dniu ogłoszenia.

W związku z potrzebą pilnego wprowadzenia projektowanych rozwiązania oraz jego znaczeniem dla gospodarki, zdecydowano się skorzystać z przewidzianej w art. 4 ust. 2 ustawy z dnia 20 lipca 2000 r. o ogłaszaniu aktów normatywnych i niektórych innych aktów prawnych (Dz. U. z 2019 r. poz. 1461) możliwości skrócenia *vacatio legis*. Zgodnie z ww. przepisem w uzasadnionych przypadkach akty normatywne mogą wchodzić w życie w terminie krótszym niż czternaście dni, a jeżeli ważny interes państwa wymaga natychmiastowego wejścia w życie aktu normatywnego i zasady demokratycznego państwa prawnego nie stoją temu na przeszkodzie, dniem wejścia w życie może być dzień ogłoszenia tego aktu w dzienniku urzędowym.

Informacje dodatkowe

Projekt ustawy nie zawiera przepisów technicznych i w związku z tym nie podlega procedurze notyfikacji w rozumieniu przepisów rozporządzenia Rady Ministrów z dnia 23 grudnia 2002 r. w sprawie sposobu funkcjonowania krajowego systemu notyfikacji norm i aktów prawnych (Dz. U. poz. 2039 oraz z 2004 r. poz. 597).

Stosownie do postanowień art. 5 ustawy z dnia 7 lipca 2005 r. o działalności lobbingskiej w procesie stanowienia prawa (Dz. U. z 2017 r. poz. 248) projekt został udostępniony w Biuletynie Informacji Publicznej. Ponadto, zgodnie z § 52 ust. 1 uchwały nr 190 Rady Ministrów z dnia 29 października 2013 r. – Regulamin pracy Rady Ministrów (M.P. z 2022 r. poz. 348), został udostępniony w Biuletynie Informacji Publicznej na stronie podmiotowej Rządowego Centrum Legislacji, w serwisie Rządowy Proces Legislacyjny.

Projektowane regulacje nie stoją w sprzeczności z prawem Unii Europejskiej.

Projekt nie wymaga zasięgnięcia opinii, dokonania konsultacji oraz uzgodnienia z właściwymi organami i instytucjami Unii Europejskiej, w tym Europejskim Bankiem Centralnym.

<p>Nazwa projektu Ustawa o zmianie niektórych ustaw w celu rozwoju usług cyfrowych</p> <p>Ministerstwo wiodące i ministerstwa współpracujące Ministerstwo Cyfryzacji</p> <p>Osoba odpowiedzialna za projekt w randze Ministra, Sekretarza Stanu lub Podsekretarza Stanu Paweł Lewandowski, Podsekretarz Stanu w Ministerstwie Cyfryzacji</p> <p>Kontakt do opiekuna merytorycznego projektu Maciej Górski, maciej.gorski@cyfra.gov.pl</p>	<p>Data sporządzenia 01.12.2023 r.</p> <p>Źródło: Inne</p> <p>Nr w wykazie prac legislacyjnych i programowych Rady Ministrów UD7</p>
---	---

OCENA SKUTKÓW REGULACJI

1. Jaki problem jest rozwiązywany?

Celem projektowanej ustawy jest wprowadzenie podstaw prawnych dla funkcjonowania rozwiązań usprawniających oraz rozwijających funkcjonowanie e-administracji, w zakresie dostarczania obywatelom usług cyfrowych. Intensywny proces transformacji cyfrowej polskiej administracji wymaga dostosowania otoczenia prawnego do dynamicznie zmieniającej się rzeczywistości. W 2008 r. została wprowadzona platforma ePUAP i istnieje potrzeba jej ciągłej modernizacji, jak również innych systemów służących do zapewniania nowoczesnych e-usług obywatelom. Zaproponowane rozwiązania poprawią proces rozwoju usług wprowadzając nowy dokument strategiczny oraz nowe podstawy prawne udostępniania e-usług.

2. Rekomendowane rozwiązanie, w tym planowane narzędzia interwencji, i oczekiwany efekt

Ustawa wprowadza:

- cyfrowe świadectwo rzeczoznawcy majątkowego wydawanego w oparciu o udostępnianą elektronicznie fotografię z Rejestru Dowodów Osobistych, które będzie dostępne również w aplikacji mObywatel,
- przepisy umożliwiające tworzenie zaawansowanych (dojrzałych) usług cyfrowych, m.in. w serwisie internetowym mObywatel.gov.pl,
- nowy dokument charakterze strategicznym w dziedzinie informatyzacji państwa, który pozwoli na sprawniejsze wydatkowanie środków Unii Europejskiej na informatyzację, dzięki poprawie procesu planowania działań,
- przeciwdziałanie kradzieżom tożsamości przez udostępnianie wizerunku z Rejestru Dowodów Osobistych, co ograniczy używanie fałszywych dowodów osobistych,
- Rejestr Pełnomocnictw Elektronicznych ułatwiający załatwianie spraw urzędowych przez pełnomocnika,
- nowy maksymalny termin wdrożenia systemu e-Doręczeń,
- rozszerzenie zbioru narzędzi do weryfikacji użytkowników aplikacji mObywatel o usługę online, tj. weryfikator w wersji webowej.

3. Jak problem został rozwiązany w innych krajach, w szczególności krajach członkowskich OECD/UE?

Nie dotyczy.

4. Podmioty, na które oddziałuje projekt

Grupa	Wielkość	Źródło danych	Oddziaływanie
Obywatele	Osoby w wieku produkcyjnym i poprodukcyjnym: ok. 31 milionów	Rocznik Statystyczny GUS 2022	Zwiększenie dostępności usług cyfrowych świadczonych przez administrację.
Rzecznawcy majątkowi	ok. 8200	Centralny Rejestr Rzecznawców Majątkowych	Ułatwienie w zakresie uzyskiwania świadectwa rzeczoznawcy majątkowego.
Poczta Polska	1		Możliwość korzystania z pełnomocnictw pocztowych udzielanych za pośrednictwem Rejestru Pełnomocnictw Elektronicznych.

Zawody zaufania publicznego	69756	Statystyki własne Ministerstwa Cyfryzacji prowadzone na potrzeby monitorowania statusu wdrożenia doręczeń elektronicznych	Przesunięcie terminu wdrożenia doręczeń elektronicznych zapewni więcej czasu na dostosowanie techniczne i organizacyjne do nowego sposobu prowadzenia korespondencji z podmiotami publicznymi.
Banki (komercyjne, spółdzielcze, państwowe) i SKOK (Spółdzielcze Kasy Oszczędnościowo-Kredytowe)	ok. 600	Analiza własna	Podniesienie poziomu bezpieczeństwa.
Obywatele	Przedsiębiorcy: ok. 4 828 660	Podmioty gospodarki zarejestrowane w rejestrze REGON, deklarujące prowadzenie działalności – 4 282 660 – na terenie całego kraju (dane na dzień 31.12.2022 r.)	Przesunięcie terminu wdrożenia doręczeń elektronicznych zapewni więcej czasu na dostosowanie techniczne i organizacyjne do nowego sposobu prowadzenia korespondencji z podmiotami publicznymi.
Podmioty sektora publicznego	ok. 68 000	Informacje o liczbie podmiotów – według stanu rejestru REGON na dzień 30 czerwca 2017 r.	Przesunięcie terminu wdrożenia doręczeń elektronicznych zapewni więcej czasu na dostosowanie techniczne i organizacyjne do nowego sposobu prowadzenia korespondencji z podmiotami publicznymi oraz podmiotami niepublicznymi.
Operator wyznaczony – Poczta Polska S.A.	Przedsiębiorca o ogólnopolskim zasięgu działania zatrudniający ok. 80 000 osób	Raport UKE o stanie rynku pocztowego w 2017 r	Przesunięcie terminu wejścia w życie obowiązku umożliwi Operatorowi wyznaczonemu na dostosowanie do nowych zapisów Standardu usługi rejestrowanego doręczenia elektronicznego.

5. Informacje na temat zakresu, czasu trwania i podsumowanie wyników konsultacji

Stosownie do postanowień art. 5 ustawy z dnia 7 lipca 2005 r. o działalności lobbingsowej w procesie stanowienia prawa, projekt został udostępniony w Biuletynie Informacji Publicznej. Ponadto zgodnie z § 52 ust. 1 uchwały nr 190 Rady Ministrów z dnia 29 października 2013 r. – Regulamin pracy Rady Ministrów, projekt został udostępniony w Biuletynie Informacji Publicznej na stronie podmiotowej Rządowego Centrum Legislacji, w serwisie Rządowy Proces Legislacyjny. Projekt jest odpowiedzią na postulaty organizacji zrzeszających m.in. jednostki samorządu terytorialnego, czy zawody zaufania publicznego oraz innych interesariuszy. W celu weryfikacji przedstawionych przez te podmioty obaw w Ministerstwie Cyfryzacji zorganizowano spotkanie konsultacyjne, które odbyło się w formule hybrydowej 22 listopada 2023 r. Podczas spotkania przedstawiciele ww. organizacji potwierdzili potrzebę wydłużenia terminu wprowadzenia obowiązku stosowania doręczeń elektronicznych, co pozwoli na lepsze przygotowanie do stosowania wprowadzanych ustawą rozwiązań w obszarze komunikacji elektronicznej.

6. Wpływ na sektor finansów publicznych

(ceny stałe z r.)	Skutki w okresie 10 lat od wejścia w życie zmian [mln zł]											
	0	1	2	3	4	5	6	7	8	9	10	Łącznie (0-10)
Dochody ogółem	0	0	0	0	0	0	0	0	0	0	0	0
budżet państwa	0	0	0	0	0	0	0	0	0	0	0	0
JST	0	0	0	0	0	0	0	0	0	0	0	0

pozostałe jednostki (oddzielnie)	0	0	0	0	0	0	0	0	0	0	0	0
Wydatki ogółem	0	0	0	0	0	0	0	0	0	0	0	0
budżet państwa	0	0	0	0	0	0	0	0	0	0	0	0
JST	0	0	0	0	0	0	0	0	0	0	0	0
pozostałe jednostki (oddzielnie)	0	0	0	0	0	0	0	0	0	0	0	0
Saldo ogółem	0	0	0	0	0	0	0	0	0	0	0	0
budżet państwa	0	0	0	0	0	0	0	0	0	0	0	0
JST	0	0	0	0	0	0	0	0	0	0	0	0
pozostałe jednostki (oddzielnie)	-	-	-	-	-	-	-	-	-	-	-	-
Źródła finansowania					Część 27 budżetu państwa - informatyzacja							
Dodatkowe informacje, w tym wskazanie źródeł danych i przyjętych do obliczeń założeń					Projektowane zmiany nie wywołują skutków finansowych – minister właściwy do spraw informatyzacji zabezpieczył adekwatne środki finansowe w ramach części 27 budżetu państwa w celu rozwoju serwisu internetowego mObywatel oraz aplikacji mObywatel.							
7. Wpływ na konkurencyjność gospodarki i przedsiębiorczość, w tym funkcjonowanie przedsiębiorców oraz na rodzinę, obywateli i gospodarstwa domowe												
Skutki												
Czas w latach od wejścia w życie zmian	0		1	2	3	5	10		<i>Łącznie (0-10)</i>			
W ujęciu pieniężnym (w mln zł, ceny stałe z r.)	duże przedsiębiorstwa		Brak danych									
	sektor mikro-, małych i średnich przedsiębiorstw		Brak danych									
	rodzina, obywatele oraz gospodarstwa domowe		Brak danych									
W ujęciu niepieniężnym	duże przedsiębiorstwa		Przesunięcie terminu wdrożenia doręczeń elektronicznych zapewni więcej czasu na dostosowanie techniczne i organizacyjne do nowego sposobu prowadzenia korespondencji z podmiotami publicznymi i docelowo zmniejszenie kosztów korespondencji.									
	sektor mikro-, małych i średnich przedsiębiorstw		Przesunięcie terminu wdrożenia doręczeń elektronicznych zapewni więcej czasu na dostosowanie techniczne i organizacyjne do nowego sposobu prowadzenia korespondencji z podmiotami publicznymi i docelowo zmniejszenie kosztów korespondencji.									
	rodzina, obywatele oraz gospodarstwa domowe		Przesunięcie terminu wdrożenia doręczeń elektronicznych zapewni więcej czasu na dostosowanie techniczne i organizacyjne do nowego sposobu prowadzenia korespondencji z podmiotami publicznymi i docelowo zmniejszenie kosztów korespondencji.									
	(dodaj/usuń)											

Niemierzalne	(dodaj/usuń)	
	(dodaj/usuń)	
Dodatkowe informacje, w tym wskazanie źródeł danych i przyjętych do obliczeń założeń		
8. Zmiana obciążeń regulacyjnych (w tym obowiązków informacyjnych) wynikających z projektu		
nie dotyczy		
Wprowadzane są obciążenia poza bezwzględnie wymaganymi przez UE (szczegóły w odwróconej tabeli zgodności).	tak nie nie dotyczy	
zmniejszenie liczby dokumentów zmniejszenie liczby procedur skrócenie czasu na załatwienie sprawy inne:	zwiększenie liczby dokumentów zwiększenie liczby procedur wydłużenie czasu na załatwienie sprawy inne:	
Wprowadzane obciążenia są przystosowane do ich elektroniczności.	tak nie nie dotyczy	
Komentarz:		
9. Wpływ na rynek pracy		
Brak wpływu.		
10. Wpływ na pozostałe obszary		
środowisko naturalne sytuacja i rozwój regionalny sądy powszechne, administracyjne lub wojskowe	demografia mienie państwowe inne:	informatyzacja zdrowie
Omówienie wpływu	Projekt przyspieszy transformację cyfrową administracji oraz zapewni wzrost bezpieczeństwa w objętych regulacją podmiotach.	
11. Planowane wykonanie przepisów aktu prawnego		
Ustawa wchodzi w życie po upływie 14 dni od dnia ogłoszenia, z wyjątkiem: 1) art. 1 i art. 3 pkt 4 w zakresie art. 19ab ust. 1 pkt 3 i art. 19ac, które w które wychodzą w życie z dniem określonym w komunikacie, o którym mowa w art. 11; 2) art. 2 pkt 2, który wchodzi w życie z dniem określonym w komunikacie, o którym mowa w art. 12; 3) art. 3 pkt 2, który wchodzi w życie z dniem 1 stycznia 2025 r.; 4) art. 4 pkt 2 i 3, które wchodzi w życie z dniem określonym w komunikacie, o którym mowa w art. 13; 5) art. 7, który wchodzi w życie z dniem następującym po dniu ogłoszenia.		
12. W jaki sposób i kiedy nastąpi ewaluacja efektów projektu oraz jakie mierniki zostaną zastosowane?		
Nie dotyczy.		
13. Załączniki (istotne dokumenty źródłowe, badania, analizy itp.)		
Załącznik 1. Ocena skutków dla ochrony danych -RPE Załącznik 2. Ocena skutków dla ochrony danych -udostępnianie wizerunku z RDO		

NAZWA PROCESU LUB PROJEKTU PODLEGAJĄCEGO OCENIE		Rejestr Pełnomocnictw Elektronicznych
SZCZEGÓŁOWY OPIS PROJEKTU		
#	TREŚĆ PYTANIA	
1	Opis operacji oraz charakteru przetwarzania danych (należy m.in. wskazać, czy zachodzi profilowanie lub zautomatyzowane podejmowanie decyzji)	Przeznaczeniem rejestru jest gromadzenie informacji o pełnomocnictwach udzielanych między osobami fizycznymi posiadającymi numer PESEL. W zakresie pełnomocnictw elektronicznych rejestr ten będzie rejestrem referencyjnym dla innych systemów administracji publicznej. W prowadzenie rejestru sankcjonuje również możliwość posługiwania się odpisem danych o pełnomocnictwie elektronicznym, przechowywanym w ramach tego rejestru. Rejestr udostępnił będzie usługę weryfikacji danych o pełnomocnictwie elektronicznym. Z punktu widzenia Użytkownika, wprowadzany rejestr pozwoli na zarządzanie wszystkimi pełnomocnictwami elektronicznymi z poziomu jednego punktu dostępu oraz zagwarantuje mu pewność honorowania takiego pełnomocnictwa przez wszystkie organy państwowe oraz prywatne realizujące zadania publiczne. Rejestr Pełnomocnictw Elektronicznych (RPE) przetwarza następujące dane osobowe: PESEL, Nazwisko, Imię. Operacja przetwarzania danych dotyczy usługi tworzenia Pełnomocnictwa – dokumentu, który będzie zawierał dane osobowe Mocodawcy i Pełnomocnika. Dane osobowe są wprowadzone tylko przez użytkownika (Mocodawcę) w aplikacji mObywatel i trafiają do RPE, gdzie są przechowywane. Podstawowe operacje systemu RPE podzielone są na trzy grupy: 1. Operacje w aplikacji mObywatel - tworzenie danych 2. Operacje Rejestru - zapisywanie danych - odczytywanie danych - aktualizowanie danych - usuwanie danych (błędnych i podlegających retencji) 3. Operacje backend - pobieranie danych osobowych z SRP - generowanie dokumentów .pdf na podstawie danych gromadzonych w Rejestrze - weryfikacja danych osobowych poprzez wewnętrzny System (Źródło) w Urzędach - weryfikacja danych osobowych w systemach zewnętrznych poprzez usługę publiczną Usługa nie zakłada profilowania, ani nie wykorzystuje silników procesowych do automatyzacji podejmowanych decyzji.
2	Cele przetwarzania danych osobowych	Celem przetwarzania danych jest: utworzenie dokumentu Pełnomocnictwa, który będzie przetwarzany i udostępniany w ramach RPE. W przypadku zmiany nazwiska lub imienia w rejestrze PESEL te dane w RPE są automatycznie aktualizowane w oparciu o usługę subskrypcji SRP. Gromadzenie pełnomocnictw udzielonych przez uwierzytelnionego użytkownika osobie fizycznej posiadającej numer PESEL (pełnomocnictwa elektroniczne). Pobranie z rejestru odpisu pełnomocnictwa (inne pełnomocnictwo o treści ustalonej przez mocodawcę) opatrzzonego kwalifikowaną pieczęcią elektroniczną ministra właściwego do spraw informatyzacji.
3	Podstawy prawne przetwarzania danych osobowych (w tym profilowania oraz automatycznego podejmowania decyzji)	Art. 8 pkt. 13 projektowanej ustawy o zmianie niektórych ustaw w związku z rozwojem e-administracji dodający art.19ac do ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne; Art. 1 projektowanej ustawy o zmianie niektórych ustaw w związku z rozwojem e-administracji dodający w art. 33 § 5 i 6 do ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego.
4	Opis prawnie uzasadnionych interesów realizowanych przez administratora (w przypadku, gdy podstawą przetwarzania jest uzasadniony interes administratora)	Nie dotyczy
5	Kategorie podmiotów, których dane są przetwarzane	Obywatel korzystający z usługi RPE Urzednik weryfikujący dane osobowe
6	Kategorie danych osobowych, które są przetwarzane	Dane osobowe: PESEL, nazwisko, imię
7	Źródło pochodzenia danych (należy wskazać, czy dane pochodzą od podmiotu danych, czy są pozyskiwane z innych źródeł)	Dane pochodzą od podmiotu wprowadzającego dane i ich zgodność w zakresie imię, nazwisko, PESEL jest weryfikowana automatycznie (na podstawie usługi subskrypcji) z rejestrem PESEL.
8	Podmioty, którym administrator powierza przetwarzanie danych osobowych	W zakresie utrzymania systemu: Centralny Ośrodek Informatyki Aleje Jerozolimskie 132-136 02-305 Warszawa email: coi@coi.gov.pl
9	Podstawa prawna powierzenia danych	Umowa powierzenia przetwarzania danych osobowych z COI.
10	Podmioty, którym administrator udostępnia dane osobowe	Dane osobowe mogą być przekazywane: Podmiotom wnioskujących o dostęp po uzyskaniu zgody ministra właściwego do spraw informatyzacji na potwierdzenie Pełnomocnictwa
11	Podstawa prawna udostępnienia danych przez administratora	Art. 8 pkt. 13 projektowanej ustawy o zmianie niektórych ustaw w związku z rozwojem e-administracji dodający art. 19 ac ust. 9 oraz 12 do ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne;
12	Współadministratorzy danych	n/d
13	Odbiorcy danych poza Europejskim Obszarem Gospodarczym	n/d
14	Podstawa prawna transferu danych poza EOG	n/d
OPIS ZASOBÓW WYKORZYSTYWANYCH DO PRZETWARZANIA DANYCH		
#	Ocena skutków	TREŚĆ PYTANIA
1		Sprzęt wykorzystywany do przetwarzania danych osobowych (np. sprzęt komputerowy, sieć)
2		Systemy informatyczne (oprogramowanie) wykorzystywane do przetwarzania danych osobowych
		- komputer/urządzenia mobilne Mocodawcy i Pełnomocnika oraz Weryfikatora, - komputery w podmiotach realizujących sprawy zawarte w Pełnomocnictwie, - infrastruktura serwerowa niezbędna do świadczenia usługi. - aplikacja mObywatel - system RPE/ Rejestr Pełnomocnictw Elektronicznych - system Źródło - strona web do weryfikacji Pełnomocnictw
ORGANIZACYJNE ŚRODKI OCHRONY DANYCH OSOBOWYCH		
#	TREŚĆ PYTANIA	
1	Polityki/procedury wewnętrzne wdrożone przez administratora (przykładowa lista środków ochrony danych osobowych została załączona do Instrukcji korzystania z formularza oceny DPIA)	Polityka Bezpieczeństwa dla systemu Rejestr Pełnomocnictw Elektronicznych (w przygotowaniu) Polityka Bezpieczeństwa Informacji dla systemu mObywatel
2	Przyjęte kodeksy dobrych praktyk	n/d

3	<p>Przyjęte certyfikaty w zakresie bezpieczeństwa informacji (np. certyfikat bezpieczeństwa informacji 27001, certyfikat CISA - Certified Information Systems Auditor, certyfikat C/ISSP - Certified Information Systems Security Professional itp.)</p>	brak
---	--	------

FIZYCZNE ORAZ TECHNICZNE ŚRODKI OCHRONY DANYCH OSOBOWYCH

#	TREŚĆ PYTANIA	
1	Środki fizyczne oraz techniczne	<p>COI - struktura organizacyjna Departament Bezpieczeństwa COI na podstawie oceny bieżących zagrożeń oraz monitorowania stanu bezpieczeństwa zasobów chronionych, podejmuje działania mające na celu minimalizację ryzyk, a także ustala adekwatne do nich mechanizmy zabezpieczeń.</p> <p>W COI funkcjonują regulacje dotyczące nadawania i odbierania uprawnień do obiektów fizycznych. Wydawanie kart dostępu do stref podlegających szczególnej ochronie jest ściśle nadzorowane i rozliczane. Dostępny nadawane są na podstawie imiennych wniosków akceptowanych i zatwierdzanych przez przełożonych (kierujących komórką organizacyjną).</p> <p>Zasady ciągłości działania opisane są w Polityce Zarządzania Ciągłością Działania COI - uwzględniają szczególne uwarunkowania wynikające z funkcjonowania środowiska teleinformatycznego oraz przetwarzanych danych W przypadku wystąpienia sytuacji kryzysowej powołany jest Sztab Kryzysowy COI w ramach którego zostają uruchomione struktury Zarządzania Kryzysowego.</p> <p>Funkcjonujące w COI struktury Zarządzania Kryzysowego koordynują działania w sytuacjach wymagających uruchomienia PZCD w przypadku zagrożenia ciągłości operacyjnej, przejmując zarządzanie incydentem i dostępnymi zasobami w celu odtworzenia środowiska w lokalizacji zapasowej.</p> <p>Środki techniczne Pełnomocnictwa elektroniczne opatruje się: 1) kwalifikowanym podpisem elektronicznym albo 2) podpisem zaufanym, albo 3) podpisem osobistym, albo 4) podpisem elektronicznym weryfikowanym przy użyciu certyfikatu użytkownika publicznej aplikacji mobilnej.</p> <p>Przechowywanie kluczy i certyfikatów w sprzętowych modułach bezpieczeństwa HSM "CryptoServer CP5".</p> <p>Dostęp do danych tylko dla uwierzytelnionego użytkownika i autoryzacji zakresu dostępu z wykorzystaniem zasady minimalnego dostępu. Udostępnienie danych użytkownikowi aplikacji jest każdorazowo zapisywane w dzienniku zdarzeń.</p> <p>Centra przetwarzania danych pracują w trybie Active-Active w warstwie aplikacyjnej, oraz Active-Pasive w warstwie bazodanowej. Przełączenie w przypadku awarii bazy danych wykonywane jest ręcznie zgodnie z obowiązującymi procedurami.</p> <p>Bezpieczeństwo sieci i usług sieciowych zostało zapewnione na poziomie warstwy brzegowej w oparciu o rozwiązania klasy wykorzystujące mechanizmy zarządzania zagrożeniem sieciowym takie jak: Firewall IPS, IDS, Proxy, Load balancer czy też DAM w warstwie danych.</p>

OCENA NIEZBĘDNOŚCI I PROPORCJONALNOŚCI ŚRODKÓW OCHRONY

NAZWA PROCESU LUB PROJEKTU PODLEGAJĄCEGO OCENIE

ŚRODKI PRZYCZYNIAJĄCE SIĘ DO ZGODNOŚCI PRZETWARZANIA Z ZASADAMI OGÓLNYMI RODO RPE

#	TREŚĆ PYTANIA	OPIS PLANOWANYCH ŚRODKÓW ORGANIZACYJNYCH I TECHNICZNYCH	OCENA ADEKWATNOŚCI ŚRODKÓW ORAZ ZALECENIA WDROŻENIA DODATKOWYCH ŚRODKÓW	WDROŻONE ŚRODKI LUB UZASADNIENIE BRAKU WDROŻENIA
1	Środki podjęte w celu zapewnienia legalności przetwarzania danych osobowych	1. Podstawą prawną przetwarzania danych osobowych jest Ustawa o zmianie niektórych ustaw w związku z rozwojem e-administracji Ustawa o informatyzacji podmiotów realizujących zadania publiczne, art. 20aa, art. 19ac. 2. Kodeks Postępowania Administracyjnego	Podstawa prawna określona ustawowo jest wystarczająca.	Nowelizacja ustaw: - o informatyzacji działalności podmiotów realizujących zadania publiczne - kodeks postępowania administracyjnego
2	Środki podjęte w celu zapewnienia zasady ograniczenia celu przetwarzania danych osobowych	Rejestr Pełnomocnictw Elektronicznych będzie przetwarzać dane w celach zgodnych z ustawą, czyli zapewnienie informacji o pełnomocnictwach udzielanych między osobami fizycznymi posiadającymi numer PESEL.	W zakresie pełnomocnictw elektronicznych rejestr ten będzie rejestrem referencyjnym dla innych systemów administracji publicznej. Wprowadzenie rejestru sankcjonuje również możliwość posługiwania się odpisem danych o pełnomocnictwie elektronicznym, przechowywanym w ramach tego rejestru. Rejestr udostępnił będzie usługę weryfikacji danych o pełnomocnictwie elektronicznym. Z punktu widzenia Użytkownika, wprowadzany rejestr pozwoli na zarządzanie wszystkimi pełnomocnictwami elektronicznymi z poziomu jednego punktu dostępu oraz zagwarantuje mu pewność honorowania takiego pełnomocnictwa przez wszystkie organy państwowe oraz prywatne realizujące zadania publiczne	Założenie rejestru jego funkcjonalności, pokrywają się z ustawą.
3	Środki podjęte w celu zapewnienia zasady minimalizacji danych osobowych	Dane przetwarzane w RPE określa ustawa i są one zgodne z zasadą minimalizacji czyli niezbędne do realizacji celu przetwarzania. Dodatkowo aby uwierzytelnić osobę pełnomocnictwa elektroniczne opatruje się: 1) kwalifikowanym podpisem elektronicznym albo 2) podpisem zaufanym, albo 3) podpisem osobistym, albo 4) podpisem elektronicznym weryfikowanym przy użyciu certyfikatu użytkownika publicznej aplikacji mobilnej.	Zakres danych jest adekwatny do realizacji celu, czyli pozwala uwierzytelnić osobę poprzez zalogowanie się do usługi jak i zweryfikować jej tożsamość, rozpocząć proces nadawania pełnomocnictwa elektronicznego jak i nanieść na nie podpis.	Działanie zgodnie z przepisami prawa
4	Środki podjęte w celu zapewnienia zasady ograniczenia czasowego	Mocodawca w każdym momencie może odwołać udzielone pełnomocnictwo. W przypadku śmierci mocodawcy lub pełnomocnika minister właściwy do spraw informatyzacji oznacza pełnomocnictwa znajdujące się w rejestrze, z adnotacją o śmierci tej osoby. Planowany jest ustawowy zapis o wyczyszczeniu przechowywaniu danych.		
ŚRODKI PRZYCZYNIAJĄCE SIĘ DO ZACHOWANIA PRAW OSÓB, KTÓRYCH DANE DOTYCZĄ				
#	TREŚĆ PYTANIA	OPIS PLANOWANYCH ŚRODKÓW ORGANIZACYJNYCH I TECHNICZNYCH	OCENA ADEKWATNOŚCI ŚRODKÓW ORAZ ZALECENIA WDROŻENIA DODATKOWYCH ŚRODKÓW	WDROŻONE ŚRODKI LUB UZASADNIENIE BRAKU WDROŻENIA

dane zgodnie z RODO możemy przetwarzać przez czas niezbędny do realizacji celu.

Co jeśli nie umieram i nie odwołuje pełnomocnictwa? Wówczas sam dokument i zawarte tam moje dane będą przetwarzane przez okres...??

Patrz co oznacza przetwarzanie: przetwarzanie" oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie;

Logi są przechowywane przez

1	Środki podjęte w celu realizacji obowiązków informacyjnych w stosunku do osoby, której dane dotyczą (art. 12, 13 i 14 RODO).	Klauzula informacyjna dla Pełnomocnictwa jest opublikowana pod adresem https://obywatel.gov.pl/rodo oraz w aplikacji mObywatel w sekcji Informacje prawne -> Polityka prywatności jest sekcja „Przetwarzanie, bezpieczeństwo, przechowywanie i pobieranie danych” Dodatkowo informacja o obowiązkach informacyjnych zostanie ujęta w przygotowywanym regulaminie korzystania z usług opartych o system Rejestr Pełnomocnictw Elektronicznych .		
2	Środki podjęte w celu realizacji prawa dostępu do danych osobowych (art. 15 ust. 1 RODO)	Osoba logując się do RPE będzie miała wgląd w swoje pełnomocnictwa i dane w nich zamieszczone o czym mowa w art. 8 pkt. 13 projektowanej ustawy o zmianie niektórych ustaw w związku z rozwojem e-administracji dodający art.19ac ust. 15 do ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne; Dodatkowo Minister Właściwy ds. Cyfryzacji będzie tradycyjnie realizował wnioski o dostęp do danych.	Przyjęte środki są adekwatne. Obecne rozwiązania pozwalają realizować prawo dostępu do danych. Warunkiem jest weryfikacja tożsamości osoby która zgłasza się z żądaniem, tak aby ADO miał 100 % pewność, że odpowiada osobie za którą podaje się nadawca żądania. Jednocześnie użytkownik może samodzielnie sprawdzić jakie dane są przetwarzane w RPE, po zalogowaniu się do rejestru.	n/d
3	Środki podjęte w celu realizacji prawa do uzyskania kopii danych (art. 15 ust. 3 RODO)	Osoba logując się do RPE będzie miała możliwość sporządzenia kopii swojego pełnomocnictwa o czym mowa w art. 8 pkt. 13 projektowanej ustawy o zmianie niektórych ustaw w związku z rozwojem e-administracji dodający art.19ac ust. 15 do ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne; Dodatkowo Minister Cyfryzacji będzie tradycyjnie realizował wnioski o kopię do danych.	Przyjęte środki są adekwatne. Obecne rozwiązania pozwalają realizować prawo do kopii danych. Warunkiem jest weryfikacja tożsamości osoby która zgłasza się z żądaniem, tak aby ADO miał 100 % pewność, że odpowiada osobie za którą podaje się nadawca żądania. Jednocześnie użytkownik może samodzielnie sprawdzić jakie dane są przetwarzane na jego koncie, po zalogowaniu się do rejestru, po czym wykonać kopię pełnomocnictwa.	n/d
4	Środki podjęte w celu realizacji prawa do przenoszenia danych (art. 20 RODO)	Nie dotyczy, ponieważ prawo do przenoszenia przysługuje, gdy przetwarzanie jest oparte na zgodzie (art. 6 ust. 1 lit. a RODO) lub umowie (art. 6 ust. 1 lit. b RODO), natomiast RPE będzie uregulowany ustawowo czyli przetwarzanie będzie niezbędne do realizacji obowiązku prawnego ciążącego na administratorze (art. 6 ust. 1 lit c RODO).	n/d	n/d
5	Środki podjęte w celu realizacji prawa do sprostowania (art. 16 i 19 RODO)	System aplikacji umożliwia realizację prawa do sprostowania, co zostało opisane w regulaminach usług.	Przyjęte środki są adekwatne, zapewniają i dają możliwość zapewnienia tego prawa przez osobę, której dane dotyczą.	W ramach usług w aplikacji obywatel ma prawo zgłosić nieprawidłowości do właściwego administratora. Jednocześnie w ramach poszczególnych usług w aplikacji przyjęte są rozwiązania pozwalające na samodzielne sprostowanie przez użytkownika jego danych.
6	Środki podjęte w celu realizacji prawa do usunięcia danych (do bycia zapomnianym) (art. 17 i 19 RODO)	Planowane zmiany w ustawie o zmianie niektórych ustaw w związku z rozwojem e-administracji Ustawa o informatyzacji podmiotów realizujących zadania publiczne, art. 20aa. , art. 19ac w celu uregulowania braku usuwania danych.	n/d	n/d
7	Środki podjęte w celu realizacji prawa do ograniczenia przetwarzania (art. 18 i 19 RODO)	Nie dotyczy. Katalog danych określa ustawa i są one niezbędne do utworzenia pełnomocnictwa elektronicznego, jakiegokolwiek ograniczenie danych nie będzie pozwalało na korzystanie z usługi.	n/d	n/d
8	Środki podjęte w celu realizacji prawa do wyrażenia sprzeciwu (art. 21 RODO)	Nie dotyczy, ponieważ prawo jest zarezerwowane dla przetwarzania na podstawie: - art. 6 ust. 1 lit. e (przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi) lub - art. 6 ust. 1 lit. f (prawnie uzasadniony interes) Natomiast RPE jest oparty na art. 6 ust. 1 lit. c (przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze).	n/d	n/d

METODA OCENY RYZYKA POTENCJALNEGO ORAZ SZCZĄTKOWEGO

ISTOTNOŚĆ (WAGA) ZAGROŻENIA	PRAWDOPODOBIENSTWO WYSTĄPIENIA ZAGROŻENIA				
	pomijalne (1)	niskie (2)	średnie (3)	wysokie (4)	krytyczne (5)
pomijalna (1)	1	2	3	4	5
niska (2)	2	4	6	8	10
średnia (3)	3	6	9	12	15
wysoka (4)	4	8	12	16	20
krytyczna (5)	5	10	15	20	25
STOPIEŃ RYZYKA					
	niski (1-7)	średni (8-14)	wysoki (15-25)		

SZCZEGÓLNY OPIS OPERACJI PRZETWARZANIA ORAZ ZAOSTOSOWANYCH ŚRODKÓW OCHRONY		
NAZWA PROCESU LUB PROJEKTU PODLEGAJĄCEGO OCENIE		Udostępnianie uprawnionym podmiotom wizerunku z rejestru dowodów osobistych (RDO)
SZCZEGÓLNY OPIS PROJEKTU		
#	TREŚĆ PYTANIA	ODPOWIEŹ
1	Opis operacji oraz charakteru przetwarzania danych (należy m. in. wskazać, czy zachodzi profilowanie lub automatyzowane podejmowanie decyzji)	Udostępnienie wizerunku osoby z Rejestru Dowodów Osobistych zakłada udostępnienie dla podmiotów komercyjnych, które wykazują interes faktyczny w dostępie do wizerunku oraz podmiotom powierzanym Profili Zaufania. Udostępnienie podmiotom komercyjnym następuje w trybie teletransmisji. Zgodnie z przepisami ustawy o prawie do informacji o przetwarzaniu danych w tym trybie musi zostać wydana przez ministra właściwego do spraw informatyki po zwerifikowaniu przesłanych ustawowych jak również wszelkich operacji po stronie podmiotu, któremu udostępniono dane jak i posiadania odpowiednich zabezpieczeń technicznych i organizacyjnych uniemożliwiających dostęp do danych osobom niezamierzonym. Sam proces udostępnienia wizerunku podmiotom komercyjnym następuje etapowo - w pierwszym etapie podmiot ten musi dokonać pozycyjnej weryfikacji określonych danych dowodu osobistego i danych osoby, w drugim etapie po pozytywnej weryfikacji danych dokonywany jest następujący udostępnienie wizerunku. Tali tryb uniemożliwia pozyskiwanie wizerunku dowolnej osoby bez znajomości szczegółowych informacji dotyczących dokumentu, które pozyskiwane są w celu zwaleniwa np. umowy rachunku bankowego i zamknięcie się na dowodzie osobistym. Podmioty pełnią funkcję punktu powierzanego Profili Zaufania dostęp do wizerunku otrzymują za pośrednictwem systemu Profili Zaufania, w którym następuje powierzenie PZ (podmiotu) jak następuje do trybu wizerunku (PZ) w trybie wizerunku (PZ). Bank krajowy lub inny przedsiębiorca wykorzystujący środki identyfikacji elektronicznej stosowane do uwierzytelniania w jego systemie teleinformatycznym do powierzenia profilu zaufanego lub własnego systemu będzie mógł korzystać z usług udostępnienia wizerunku po spełnieniu wymogów określonych w ustawie o dowodach osobistych w zakresie zgodności. W analizie podmiot komercyjny, który uzyskał zgodę ministra na dostęp do usług udostępniania wizerunku może bez wymogu dla wykorzystywania usług do powierzenia Profili Zaufanego. Powierzenie PZ może bowiem odbywać się z użyciem środka identyfikacji stosowanego do uwierzytelniania w systemie teleinformatycznym podmiotu, który z kolei wywołano jest po weryfikacji tożsamości osoby i jej dokumentu w procesach związanych z działalności tych podmiotów (np. przy zakładaniu rachunku bankowego).
2	Cele przetwarzania danych osobowych	Wypracowanie procesu ponowne na zapewnienie wiarygodności informacji i ograniczenia uchyła określonych czy ofiarowanych dokumentów, zapewnia kradzieży tożsamości. Udostępnienie wizerunku jest warstwą doświadczenia, która pozwoli porównać wizerunek z dowodem osobistego który przedkłada Klient z wizerunkiem z Rejestru Dowodów Osobistych. Należy wskazać, że przetwarzanie łączy przepisy przy użyciu dokumentów dotyczący jego przebiegu w obszarze fotografii i załącznika do dokumentu oryginalnego z oryginalnym zabezpieczeniem fizycznym. Wprowadzenie nowego mechanizmu pozwalającego na identyfikację w trybie odcisków palców i danych takich jak dane biometryczne w znacznym stopniu przyczyni się do uszczelnienia takich procesów jak wydawanie środków identyfikacji elektronicznej, zawieranie umów i transakcji w obszarze teleinformatycznym czy też strona finansowa. Z punktu widzenia bezpieczeństwa PZ jako środka identyfikacji, rozwiązanie pozwoli na ograniczenie incydentów podważania się pod imię osoby i przetwarzania lub zalegania na jej dane Profili Zaufanego a także wzmocni proces weryfikacji tożsamości osoby, która potwierdzi PZ za pośrednictwem np. banku.
3	Podstawy prawne przetwarzania danych osobowych (w tym profilowanie oraz automatyzowane podejmowanie decyzji)	projektowany art. 68a projektu ustawy o zmianie niektórych ustaw w związku z rozwojem e-administracji oraz art. 9 ust. 2 lit. g RODO
4	Opis prawnie uzasadnionych interesów realizowanych przez administratora (w przypadku, gdy podmiot przetwarzający jest uzasadniony interesem administracyjnym)	Nie dotyczy
5	Kategorie podmiotów, którym dane są przetwarzane	Osoby fizyczne (obywateli polscy), którzy posiadają ważny dowód osobisty. W przypadku braku posiadania ważnego dowodu osobistego usługi weryfikacji w pierwszym kroku negatywnie dokument, co uniemożliwi udostępnienie wizerunku osoby. Aby to uszczelnienie tym, że osoba taka nie może zwracać kasałki z podmiotem komercyjnym nie posiadającym zdolności potwierdzenia tożsamości w oparciu o dowód osobisty a załem dodatkowe udostępnienie wizerunku osoby było w tej sytuacji działaniem nadmiernym.
6	Kategorie danych osobowych, które są przetwarzane	1) imię (imiona); 2) nazwisko; 3) numer PESEL; 4) data wydania dowodu osobistego; 5) data wydania dowodu osobistego; 6) termin ważności dowodu osobistego; 7) znacznik kasy.
7	Źródło pochodzenia danych (należy wskazać, czy dane pochodzą od podmiotu danych, czy są pozyskiwane z innych źródeł)	Rejestr Dowodów Osobistych, będący częścią SRP (systemu rejestrów państwowych)
8	Podmioty, którym administrator powierza przetwarzanie danych osobowych	Centrały Ośrodków Informacji
9	Podstawa prawna powierzenia danych	Umowa powierzenia przetwarzania danych osobowych z COI dnia 5 lipca 2018 r. (karta nr 3 do umowy).
10	Podmioty, którym administrator udostępnia dane osobowe	Dotyczy podmioty wskazane w art. 20c ust. 2, 3 i 8 ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne, które potwierdzają Profili Zaufania (pełnią lub mogą pełnić funkcję punktu powierzanego PZ lub powierzonego do użyciem środka identyfikacji elektronicznej do uwierzytelniania w ich systemach): 1) konsolidacja; 2) znacznik urzędu skarbowego; 3) województwo; 4) Związek Zawodowy Spółdzielców; 5) Narodowy Fundusz Zdrowia; 6) inny podmiot publiczny (definicja podmiotu publicznego w art. 2 ustawy o informatyzacji); 7) bank krajowy, o którym mowa w art. 4 ust. 1 pkt 1 ustawy z dnia 29 sierpnia 1997 r. – Prawo bankowe (Dz.U. z 2020 r. poz. 1896, z późn. zm. 9)); 8) operator pocztowy, o którym mowa w art. 4 pkt 12 ustawy z dnia 23 listopada 2012 r. – Prawo telekomunikacyjne; (Dz.U. z 2020 r. poz. 1041 i 2320); 9) oddział instytucji kredytowej, o którym mowa w art. 4 ust. 1 pkt 18 ustawy z dnia 29 sierpnia 1997 r. – Prawo bankowe; 10) spółdzielcza kasa oszczędnościowo-kredytowa, o której mowa w ustawie z dnia 5 listopada 2009 r. o spółdzielczych kasach oszczędnościowo-kredytowych (Dz.U. z 2021 r. poz. 1844) 11) bank krajowy lub inny przedsiębiorca, który posiada zgodę na nieobowiązkowe wykorzystywanie środków identyfikacji elektronicznej stosowanych do uwierzytelniania w systemie teleinformatycznym banku krajowego lub innego przedsiębiorcy do potwierdzenia tożsamości i zaufania.
11	Podstawa prawna udostępnienia danych przez administratora	projektowany art. 68a projektu ustawy o zmianie niektórych ustaw w związku z rozwojem e-administracji oraz art. 9 ust. 2 lit. g RODO
12	Współadministratorzy danych	Dane w RDO gromadzone na dotychczasowych zasadach. Nowe przepisy regulują kwestię udostępniania a nie gromadzenia danych. Podmioty, które uzyskują dane w trybie teletransmisji w wyniku udostępnienia stają się samodzielnymi administratorami danych.
13	Obiory danych poza Europejskim Obszarem Gospodarczym	Nie dotyczy
14	Podstawa prawna transferu danych poza EOG	Nie dotyczy
OPIS ZASOBÓW WYKORZYSTYWANYCH DO PRZETWARZANIA DANYCH		
#	TREŚĆ PYTANIA	OPIS
1	Sprzęt wykorzystywany do przetwarzania danych osobowych (np. sprzęt komputerowy, sieci)	Dane osobiste w trybie teletransmisji danych. Zgodnie z PBI SRP załączonym sposobem podłączenia infrastruktury interesariuszy zewnętrznych systemu jest wykorzystanie dedykowanej wydzielonej sieci teleinformatycznej będącej w gronie sieci podległych Ministerstwu właściwemu do spraw informatyki i z zachowaniem pełnej separacji sieci roboczych systemu umieszczonego w lokalizacji uprzednich interesariuszy od innych sieci. W sieci lokalnej interesariuszy również wymagana jest separacja sieci dostępnego do SRP od innych sieci urzędu. Odpowiednio od PBI wymagają podpisania umowy o udostępnienie z ministrem właściwym do spraw informatyki oraz ministrem właściwym do spraw energetyki. Na etapie zawierania umowy o udostępnienie badanie i gwarantowanie są odpowiednie środki bezpieczeństwa (mogą różnić się w zależności od interesariusza). Opis założeń sprzętowych powierzonego PBI SRP.
2	Przyjęte procedury wewnętrzne wdrożone przez administratora (np. przykładowa lista środków ochrony danych osobowych została załączona do instrukcji korzystania z formularza oceny DPIA)	Punkty powierzonego Profili Zaufania będące podmiotami publicznymi i stosujący system zarządzania bezpieczeństwem informacji zapewniający poufność, dostępność i integralność informacji zgodnie z wymogami określonymi w 20 rozporządzeniu Rady Ministrów w sprawie krajowych ram interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiaru informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U. z 2011 r. poz. 2247) i/ lub rozporządzenia KPI. Rozporządzenie Ministra Cyfryzacji z dnia 01 czerwca 2020 r. w sprawie profilu zaufanego i podpisu zaufanego (Dz.U. z 2020, poz. 1184 zm. Dz.U. z 2021, poz. 1078) w § 19 ust. 1 pkt 2 wymaga od podmiotów wykorzystujących środki identyfikacji elektronicznej stosowane do uwierzytelniania w systemie teleinformatycznym podmiotu niepublicznego do powierzenia profilu zaufanego ograniczenia, ustanowienia, wdrożenia, eksploatacji, monitorowania, przeglądu, utrzymania i doskonałości systemu zarządzania bezpieczeństwem informacji z wyjątkiem określonych w rozporządzeniu w sprawie KPI.
3	Systemy informacyjne (oprogramowanie) wykorzystywane do przetwarzania danych osobowych	System Rejestrów Państwowych - w jego ramach Rejestr Dowodów Osobistych udostępnia wizerunek (fotografię) i rzucę usług web services. Udostępnienie dane są pobierane przez system podmiotu, który posiada decyzję wyrażającą zgodę na dostęp do danych w trybie teletransmisji np. system Dokumenty Załączzone Proszonymo przez Związek Banków Polskich, który obecnie wykorzystywany jest przez większość banków w celu dostępu do usług weryfikacji danych dowodu osobistego. System Profili Zaufania - wykorzystywany przez punkty powierzonego PZ, system banku krajowego lub innego przedsiębiorcy wykorzystującego środki identyfikacji elektronicznej stosowane do uwierzytelniania w systemie teleinformatycznym banku krajowego lub innego przedsiębiorcy do powierzenia PZ.
ORGANIZACYJNE ŚRODKI OCHRONY DANYCH OSOBOWYCH		
#	TREŚĆ PYTANIA	ODPOWIEŹ
1	Polityki proceduralne wewnętrzne wdrożone przez administratora (np. przykładowa lista środków ochrony danych osobowych została załączona do instrukcji korzystania z formularza oceny DPIA)	Polityka bezpieczeństwa informacji SRP (wygłosz. https://www.gov.pl/web/ryzyki/uzyskanie-dostepu-danych-z-rejestru-pesei/) Instrukcja dla osoby powierzonego Profili Zaufania (https://mc.gov.pl/pl/interoperacyjnos-c/mwz-krajowy-dokumentacja-dotyczaca-integracji-z-wzsem-krajowym.html) Procedura użycia punktu powierzonego Profili Zaufania (https://mc.gov.pl/pl/interoperacyjnos-c/mwz-krajowy-dokumentacja-dotyczaca-integracji-z-wzsem-krajowym.html) Procedura nadawania uprawnień do obsługi punktu powierzonego Profili Zaufania (https://mc.gov.pl/pl/interoperacyjnos-c/mwz-krajowy-dokumentacja-dotyczaca-integracji-z-wzsem-krajowym.html) Audyty techniczne wdrożone i jego systemy, który będzie wykorzystywał do kontroli w trybie teletransmisji z PBI weryfikacja zgodności z SRP, weryfikacja zabezpieczeń technicznych i organizacyjnych służących do danych osobowych. Realizacja przed wydaniem decyzji wyrażającej zgodę. Polityka certyfikacji dla infrastruktury SRP (https://www.gov.pl/web/ryzyki/uzyskanie-dostepu-danych-z-rejestru-pesei/) Polityka certyfikacji dla operatorów SRP (https://www.gov.pl/web/ryzyki/uzyskanie-dostepu-danych-z-rejestru-pesei/) Polityka bezpieczeństwa dla systemu Profili Zaufania - decyzja nr 5 Ministra Cyfryzacji z dnia 27 kwietnia 2020 r. Polityka bezpieczeństwa Wzeta Krajowego (https://mc.gov.pl/pl/interoperacyjnos-c/mwz-krajowy-dokumentacja-dotyczaca-integracji-z-wzsem-krajowym.html)
2	Przyjęte kodeksy dobrych praktyk	Nie dotyczy
3	Przyjęte certyfikaty w zakresie bezpieczeństwa informacji (np. certyfikat bezpieczeństwa informacji 27001, certyfikat CISA - Certified Information Systems Auditor, certyfikat CISP - Certified Information Systems Security Professional (Ip.))	Pracownicy podmiotu utrzymującego SRP (COI) posiadają następujące certyfikaty: - CISA - CISP - ISO/IEC 27001 Lead Auditor
FIZYCZNE ORAZ TECHNICZNE ŚRODKI OCHRONY DANYCH OSOBOWYCH		
#	TREŚĆ PYTANIA	ODPOWIEŹ
1	Środki fizyczne oraz techniczne (np. przykładowa lista środków ochrony danych osobowych została załączona do instrukcji korzystania z formularza oceny DPIA)	Zgodnie z dokumentami: Polityka bezpieczeństwa informacji SRP Instrukcja dla osoby powierzonego Profili Zaufania. Procedura użycia punktu powierzonego Profili Zaufania. Procedura nadawania uprawnień do obsługi punktu powierzonego Profili Zaufania. Audyty techniczne - przed wydaniem zgody na dostęp do usług teletransmisji wykonywany jest audyt techniczny interesariusza. Polityka certyfikacji dla operatorów SRP Polityka certyfikacji dla operatorów SRP Polityka certyfikacji - po wydaniu zgody na dostęp do usług teletransmisji danych wydawany jest certyfikat dostępny dla systemu. Polityka bezpieczeństwa dla systemu Profili Zaufania - decyzja nr 5 Ministra Cyfryzacji z dnia 27 kwietnia 2020 r. Polityka bezpieczeństwa Wzeta Krajowego

OCENA NEZBEĐNOŚCI I PROPORCJONALNOŚCI ŚRODKÓW OCHRONY				
NAZWA PROCESU LUB PROJEKTU POLEGAJĄCEGO OCENIE	Udostępnianie uprawnionym podmiotom wizerunku z rejestru dowodów osobowych (ROO)			
#	TREŚĆ PYTANIA	OPIS PLANOWANYCH ŚRODKÓW ORGANIZACYJNYCH	OCENA ADEKWATNOŚCI ŚRODKÓW ORAZ ZALECENIA	WRODZONE ŚRODKI I ICH IZOPRAWNIANIE W BIEŻĄCYM WYKONANIU
1	Środek podjęty w celu zapewnienia legalności przetwarzania danych osobowych.	Projekt ustawy o zmianie niektórych ustaw w związku z rozszerzeniem e-administracji wprowadzający zmiany w ustawie o dowodach osobistych.	Uwzględnienie interesów jednostek i interesów państwa w postaci wyłączenia z Rejestru pojazdów samochodowych jedynej kategorie pojazdów (motocykle i skutery), które nie mają możliwości wyłączenia z Rejestru pojazdów samochodowych. Zmiana przepisów o wyłączeniu z Rejestru pojazdów samochodowych jedynej kategorie pojazdów (motocykle i skutery). Zmiana przepisów o wyłączeniu z Rejestru pojazdów samochodowych jedynej kategorie pojazdów (motocykle i skutery).	Nowelizacja ustawy o dowodach osobistych.
2	Środek podjęty w celu zapewnienia zasady ograniczenia celu przetwarzania danych osobowych.	Celem przetwarzania danych określają zmiany w ustawie o dowodach osobistych. W związku z tym rodzajem danych, który wnoszą do udostępnienia wizerunku, nie jest to przetwarzanie danych osobowych. Wskazano, że w tym celu nie ma potrzeby wyłączenia z Rejestru pojazdów samochodowych jedynej kategorie pojazdów (motocykle i skutery). Wskazano, że w tym celu nie ma potrzeby wyłączenia z Rejestru pojazdów samochodowych jedynej kategorie pojazdów (motocykle i skutery).	Zastosowanie środka jest adekwatne - udostępnienie wizerunku zapewni możliwość weryfikacji autentyczności dowodu osobistego i będącego podstawą do wydania dowodu osobistego. Obecność wizerunku nie jest w porównaniu z innymi danymi w tym samym celu przetwarzania danych. Wskazano, że w tym celu nie ma potrzeby wyłączenia z Rejestru pojazdów samochodowych jedynej kategorie pojazdów (motocykle i skutery). Zmiana przepisów o wyłączeniu z Rejestru pojazdów samochodowych jedynej kategorie pojazdów (motocykle i skutery).	Zastosowanie środka: - weryfikacja celu przetwarzania danych w postaci wizerunku (jeżeli w ramach weryfikacji interesu faktycznego gromadzony jest wizerunek); - weryfikacja autentyczności dowodu osobistego i będącego podstawą do wydania dowodu osobistego; weryfikacja wizerunku i innych danych w tym samym celu przetwarzania danych; weryfikacja wizerunku i innych danych w tym samym celu przetwarzania danych; weryfikacja wizerunku i innych danych w tym samym celu przetwarzania danych.
3	Środek podjęty w celu zapewnienia zasady minimalizacji danych osobowych.	Ustawa przewiduje udostępnienie wizerunku osoby w wyniku dwustronnego zlecenia. W wizerunku danych osobowych oraz jego przesłania (imię, nazwisko, numer PESEL, seria i numer dowodu osobistego, data wydania dowodu osobistego, termin ważności dowodu osobistego); 2. Udostępnienie wizerunku osoby z pozytywnie zweryfikowanego dowodu osobistego.	Podjęcie środka w sposób adekwatny zapewnia, że wizerunek osoby nie będzie udostępniany w sytuacjach umożliwiających przetwarzanie danych osobowych. W tym celu nie ma potrzeby wyłączenia z Rejestru pojazdów samochodowych jedynej kategorie pojazdów (motocykle i skutery). Zmiana przepisów o wyłączeniu z Rejestru pojazdów samochodowych jedynej kategorie pojazdów (motocykle i skutery).	Ważną rolę w tym celu odegra wizerunek osoby, który umożliwi weryfikację danych osobowych i będzie udostępniany w tym celu. W tym celu nie ma potrzeby wyłączenia z Rejestru pojazdów samochodowych jedynej kategorie pojazdów (motocykle i skutery). Zmiana przepisów o wyłączeniu z Rejestru pojazdów samochodowych jedynej kategorie pojazdów (motocykle i skutery).
4	Środek podjęty w celu zapewnienia zasady ograniczenia czasowego.	Poślężenie się niezmierzonym osobistym niemierni udostępnienie wizerunku osoby następuje po zakończeniu przetwarzania danych osobowych i dokumentu bezopisowego w oparciu o taki dokument nie powinna zostać uwolniona weryfikacja dowodu osobistego.	Zastosowanie środka jest adekwatne. Podmiot, który dane udostępnia, nie może samowolnie udostępniać danych osobom trzecim. W tym celu nie ma potrzeby wyłączenia z Rejestru pojazdów samochodowych jedynej kategorie pojazdów (motocykle i skutery). Zmiana przepisów o wyłączeniu z Rejestru pojazdów samochodowych jedynej kategorie pojazdów (motocykle i skutery).	Po udostępnieniu danych z ROO, podmiot, który dane udostępniał, nie może samowolnie udostępniać danych osobom trzecim. W tym celu nie ma potrzeby wyłączenia z Rejestru pojazdów samochodowych jedynej kategorie pojazdów (motocykle i skutery). Zmiana przepisów o wyłączeniu z Rejestru pojazdów samochodowych jedynej kategorie pojazdów (motocykle i skutery).
ŚRODKI PRZYZNACZAJĄCE SIĘ DO ZACHOWANIA PRAW OSÓB, KTÓRYCH DANE DOTYCZA				
#	TREŚĆ PYTANIA	OPIS PLANOWANYCH ŚRODKÓW ORGANIZACYJNYCH	OCENA ADEKWATNOŚCI ŚRODKÓW ORAZ ZALECENIA	WRODZONE ŚRODKI I ICH IZOPRAWNIANIE W BIEŻĄCYM WYKONANIU
1	Środek podjęty w celu realizacji obowiązku informacyjnego w stosunku do osoby, której dane dotyczą (art. 12, 13 i 14 ROO).	W urzędach gmin, które przyjmują wnioski o wydanie dowodu osobistego, dostępne są kanały informacyjne zapewniające odpowiedź elektroniczną, w tym również informację o tym, кому mogą być udostępniane dane osobiste z ROO. Kanały zostały przygotowane przez KPMR MEDIA i są dostępne dla całego kraju. Wraz z wejściem w życie zmian zostały zakupione od informatorów o możliwości udostępnienia wizerunku określonych danych osobowych.	Obowiązek spełnienia w urzędach jest wystarczający. Przed wejściem w życie zmiany zakupiono kanały informacyjne, które umożliwią weryfikację danych osobowych i będą udostępniane w tym celu. W tym celu nie ma potrzeby wyłączenia z Rejestru pojazdów samochodowych jedynej kategorie pojazdów (motocykle i skutery). Zmiana przepisów o wyłączeniu z Rejestru pojazdów samochodowych jedynej kategorie pojazdów (motocykle i skutery).	Kanały informacyjne: - w urzędach gmin przy składowaniu wniosku o dowód osobisty; - kanały informacyjne, które umożliwią weryfikację danych osobowych i będą udostępniane w tym celu; w tym celu nie ma potrzeby wyłączenia z Rejestru pojazdów samochodowych jedynej kategorie pojazdów (motocykle i skutery). Zmiana przepisów o wyłączeniu z Rejestru pojazdów samochodowych jedynej kategorie pojazdów (motocykle i skutery).
2	Środek podjęty w celu realizacji prawa do danych osobowych (art. 15 ust. 1 ROO).	Wzruszając, że Minister Cyfryzacji nieprzetwarza dane osobiste do celów, do których są przetwarzane, z wyjątkiem odzwierciedlenia, które są przetwarzane. Minister Cyfryzacji nieprzetwarza dane osobiste do celów, do których są przetwarzane, z wyjątkiem odzwierciedlenia, które są przetwarzane.	Podjęcie środka jest adekwatne - zapewnia możliwość wyłączenia z Rejestru pojazdów samochodowych jedynej kategorie pojazdów (motocykle i skutery). Zmiana przepisów o wyłączeniu z Rejestru pojazdów samochodowych jedynej kategorie pojazdów (motocykle i skutery).	Obecnie środek jest wystarczający: - środek dotyczy danych w ROO; - brak zachowania danych w systemie Profilu Zaufanego; - udostępnienie danych w formie danych osobowych i w formie danych osobowych.
3	Środek podjęty w celu realizacji prawa do uzyskania kopii danych (art. 15 ust. 3 ROO).	Przewidywane środki są adekwatne - zapewniają możliwość wyłączenia z Rejestru pojazdów samochodowych jedynej kategorie pojazdów (motocykle i skutery). Zmiana przepisów o wyłączeniu z Rejestru pojazdów samochodowych jedynej kategorie pojazdów (motocykle i skutery).	Podjęcie środka jest adekwatne - zapewnia możliwość wyłączenia z Rejestru pojazdów samochodowych jedynej kategorie pojazdów (motocykle i skutery). Zmiana przepisów o wyłączeniu z Rejestru pojazdów samochodowych jedynej kategorie pojazdów (motocykle i skutery).	W Rejestrze Dowodów Osobistych administrator ma możliwość wyłączenia z Rejestru pojazdów samochodowych jedynej kategorie pojazdów (motocykle i skutery). Zmiana przepisów o wyłączeniu z Rejestru pojazdów samochodowych jedynej kategorie pojazdów (motocykle i skutery).
4	Środek podjęty w celu realizacji prawa do przeniesienia danych (art. 18 ROO).	Zgodnie z art. 20 ust. 3 ROO prawo do przeniesienia danych do przetwarzania, które jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powołanej administracji. Przekazywanie danych z ROO oraz w systemie Profilu Zaufanego nie ma takiego charakteru.	Podjęcie środka jest adekwatne - zapewnia możliwość wyłączenia z Rejestru pojazdów samochodowych jedynej kategorie pojazdów (motocykle i skutery). Zmiana przepisów o wyłączeniu z Rejestru pojazdów samochodowych jedynej kategorie pojazdów (motocykle i skutery).	Podjęcie środka jest adekwatne - zapewnia możliwość wyłączenia z Rejestru pojazdów samochodowych jedynej kategorie pojazdów (motocykle i skutery). Zmiana przepisów o wyłączeniu z Rejestru pojazdów samochodowych jedynej kategorie pojazdów (motocykle i skutery).
5	Środek podjęty w celu realizacji prawa do wyłączenia danych (art. 17 i 19 ROO).	Zgodnie z art. 156 ustawy o dowodach osobistych w przypadku stwierdzenia błędów lub braku danych w Rejestrze Dowodów Osobistych w interesie państwa lub w ramach sprawowania władzy publicznej powołanej administracji, w tym w szczególności w celu zapewnienia bezpieczeństwa informacji, organy właściwe do nadzoru nad przetwarzaniem danych osobowych i innych danych w tym samym celu przetwarzania danych w tym celu nie ma potrzeby wyłączenia z Rejestru pojazdów samochodowych jedynej kategorie pojazdów (motocykle i skutery). Zmiana przepisów o wyłączeniu z Rejestru pojazdów samochodowych jedynej kategorie pojazdów (motocykle i skutery).	Podjęcie środka jest adekwatne - zapewnia możliwość wyłączenia z Rejestru pojazdów samochodowych jedynej kategorie pojazdów (motocykle i skutery). Zmiana przepisów o wyłączeniu z Rejestru pojazdów samochodowych jedynej kategorie pojazdów (motocykle i skutery).	Zastosowanie środka w celu wyłączenia danych z ROO w tym celu nie ma potrzeby wyłączenia z Rejestru pojazdów samochodowych jedynej kategorie pojazdów (motocykle i skutery). Zmiana przepisów o wyłączeniu z Rejestru pojazdów samochodowych jedynej kategorie pojazdów (motocykle i skutery).
6	Środek podjęty w celu zapewnienia zasady minimalizacji danych osobowych (art. 17 i 19 ROO).	Dane w tym wizerunku, przechowywane w ROO nie są z tego samego powodu, zgodnie z art. 56 pkt 2 ustawy o dowodach osobistych. Udostępniany w protokołach reklamacyjnych wizerunek nie jest z tym samym powodu, zgodnie z art. 56 pkt 2 ustawy o dowodach osobistych. Udostępniany w protokołach reklamacyjnych wizerunek nie jest z tym samym powodu, zgodnie z art. 56 pkt 2 ustawy o dowodach osobistych.	Zastosowanie środka jest adekwatne - zapewnia możliwość wyłączenia z Rejestru pojazdów samochodowych jedynej kategorie pojazdów (motocykle i skutery). Zmiana przepisów o wyłączeniu z Rejestru pojazdów samochodowych jedynej kategorie pojazdów (motocykle i skutery).	Dane nie są udostępniane w ROO i nie są z tego samego powodu, zgodnie z art. 56 pkt 2 ustawy o dowodach osobistych. Udostępniany w protokołach reklamacyjnych wizerunek nie jest z tym samym powodu, zgodnie z art. 56 pkt 2 ustawy o dowodach osobistych.
7	Środek podjęty w celu realizacji prawa do ograniczenia przetwarzania (art. 18 i 19 ROO).	Podmiot, który dane udostępnia, nie może samowolnie udostępniać danych osobom trzecim. W tym celu nie ma potrzeby wyłączenia z Rejestru pojazdów samochodowych jedynej kategorie pojazdów (motocykle i skutery). Zmiana przepisów o wyłączeniu z Rejestru pojazdów samochodowych jedynej kategorie pojazdów (motocykle i skutery).	Zastosowanie środka jest adekwatne - zapewnia możliwość wyłączenia z Rejestru pojazdów samochodowych jedynej kategorie pojazdów (motocykle i skutery). Zmiana przepisów o wyłączeniu z Rejestru pojazdów samochodowych jedynej kategorie pojazdów (motocykle i skutery).	Dane nie są udostępniane w ROO i nie są z tego samego powodu, zgodnie z art. 56 pkt 2 ustawy o dowodach osobistych. Udostępniany w protokołach reklamacyjnych wizerunek nie jest z tym samym powodu, zgodnie z art. 56 pkt 2 ustawy o dowodach osobistych.
8	Środek podjęty w celu realizacji prawa do wyłączenia sprzeciwu (art. 21 ROO).	Podmiot, który dane udostępnia, nie może samowolnie udostępniać danych osobom trzecim. W tym celu nie ma potrzeby wyłączenia z Rejestru pojazdów samochodowych jedynej kategorie pojazdów (motocykle i skutery). Zmiana przepisów o wyłączeniu z Rejestru pojazdów samochodowych jedynej kategorie pojazdów (motocykle i skutery).	Zastosowanie środka jest adekwatne - zapewnia możliwość wyłączenia z Rejestru pojazdów samochodowych jedynej kategorie pojazdów (motocykle i skutery). Zmiana przepisów o wyłączeniu z Rejestru pojazdów samochodowych jedynej kategorie pojazdów (motocykle i skutery).	Dane nie są udostępniane w ROO i nie są z tego samego powodu, zgodnie z art. 56 pkt 2 ustawy o dowodach osobistych. Udostępniany w protokołach reklamacyjnych wizerunek nie jest z tym samym powodu, zgodnie z art. 56 pkt 2 ustawy o dowodach osobistych.

METODA OCENY RYZYKA POTENCJALNEGO ORAZ SZCZĄTKOWEGO

ISTOTNOŚĆ (WAGA) ZAGROŻENIA	PRAWDOPODOBIENSTWO WYSTĄPIENIA ZAGROŻENIA				
	pomijalne (1)	niskie (2)	średnie (3)	wysokie (4)	krytyczne (5)
pomijalna (1)	1	2	3	4	5
niska (2)	2	4	6	8	10
średnia (3)	3	6	9	12	15
wysoka (4)	4	8	12	16	20
krytyczna (5)	5	10	15	20	25
STOPIEŃ RYZYKA	niski (1-7)	średni (8-14)	wysoki (15-25)		