KAP.430.022.2020
Nr ewid. 200/2020/P/20/004/KAP

Informacja o wynikach kontroli

REALIZACJA USŁUG PUBLICZNYCH DLA OBYWATELI Z WYKORZYSTANIEM PLATFORMY ePUAP

DEPARTAMENT
ADMINISTRACJI PUBLICZNEJ

MISJĄ
Najwyższej Izby Kontroli jest dbałość o gospodarność i skuteczność w służbie publicznej dla Rzeczypospolitej Polskiej

WIZJĄ
Najwyższej Izby Kontroli jest cieszący się powszechnym autorytetem najwyższy organ kontroli państwowej, którego raporty będą oczekiwanym i poszukiwanym źródłem informacji dla organów władzy i społeczeństwa

Informacja o wynikach kontroli
Realizacja usług publicznych dla obywateli z wykorzystaniem platformy ePUAP

Dyrektor
Departamentu Administracji Publicznej

BSkwarku

Bogdan Skwarka

Zatwierdzam:
Prezes Najwyższej Izby Kontroli

Marian Banaś
Warszawa, dnia 23. 02. 2021

Najwyższa Izba Kontroli
ul. Filtrowa 57
02-056 Warszawa
T/F +48 22 444 50 00

www.nik.gov.pl

SPIS TREŚCI

WYKAZ STOSOWANYCH SKRÓTÓW, SKRÓTOWCÓW I POJĘĆ 4

1. WPROWADZENIE 5

2. OCENA OGÓLNA 7

3. SYNTEZA WYNIKÓW KONTROLI 8

4. WNIOSKI 14

5. WAŻNIEJSZE WYNIKI KONTROLI 15

5.1. Realizacja przez Ministra Cyfryzacji działań w celu zapewnienia dostępności i zwiększenia liczby e-usług dla obywateli 15
5.2. Zapewnienie przez Centralny Ośrodek Informatyki funkcjonowania platformy ePUAP oraz profilu zaufanego 37
5.3. Świadczenie przez Urzędy j.s.t usług drogą elektroniczną poprzez ePUAP 55

6. ZAŁĄCZNIKI 68

6.1. Metodyka kontroli i informacje dodatkowe 68
6.2. Analiza stanu prawnego i uwarunkowań organizacyjno-ekonomicznych 83
6.3. Wykaz aktów prawnych dotyczących kontrolowanej działalności 93
6.4. Wykaz podmiotów, którym przekazano informację o wynikach kontroli 94

Zdjęcie na okładce:
© DragonImages – stock.adobe.com

Wykaz stosowanych skrótów, skrótowców i pojęć

COI Centralny Ośrodek Informatyki. COI jest instytucją gospodarki budżetowej, nad którą nadzór w okresie objętym kontrolą sprawował Minister Cyfryzacji. Zgodnie ze statutem COI[1], przedmiotem jego podstawowej działalności jest m.in. odpłatne wykonywanie na rzecz Ministra usług w zakresie utrzymania i rozwoju systemu ePUAP, a także w zakresie obsługi Profilu Zaufanego;

EOD Elektroniczny Obieg Dokumentów;

ePUAP Elektroniczna Platforma Usług Administracji Publicznej, ogólnopolska platforma teleinformatyczna, która zapewnia ustandaryzowaną komunikację między innymi pomiędzy obywatelami a administracją samorządową oraz pomiędzy urzędami administracji publicznej;

e-usługa usługa świadczona drogą elektroniczną bez jednoczesnej obecności stron (na odległość), poprzez przekaz danych na indywidualne żądanie usługobiorcy, przesyłanej i otrzymywanej za pomocą urządzeń do elektronicznego przetwarzania;

j.s.t. jednostka samorządu terytorialnego;

MC Ministerstwo Cyfryzacji. Rozporządzeniem Rady Ministrów[2] z dnia 7 października 2020 r., z mocą od dnia 6 października 2020 r., zniesione zostało Ministerstwo Cyfryzacji, a pracownicy dotychczasowego Ministerstwa Cyfryzacji obsługujący sprawy działu informatyzacja zostali włączeni do Kancelarii Prezesa Rady Ministrów;

PZIP *lub* **Program** Program Zintegrowanej Informatyzacji Państwa;

PZ Profil Zaufany;

rozporządzenie KRI rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych[3];

SOR Strategia na rzecz Odpowiedzialnego Rozwoju do roku 2020 (z perspektywą do 2030 r.);

UM Urząd Miejski/Urząd Miasta/Urząd Miasta i Gminy;

UG Urząd Gminy

ustawa o informatyzacji ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne[4].

---

[1] § 2 ust. 2 pkt 5 lit. b i pkt 7 statutu COI, wprowadzonego zarządzeniem nr 6 Ministra Cyfryzacji z dnia 31 grudnia 2015 r. w sprawie nadania statutu instytucji gospodarki budżetowej pod nazwą „Centralny Ośrodek Informatyki" (Dz. Urz. MC z 2015 r. poz. 7, ze zm.).

[2] Dz. U. poz. 1730.

[3] Dz. U. z 2017 r. poz. 2247.

[4] Dz. U. z 2020 r. poz. 346, ze zm.

1. WPROWADZENIE

Pytanie definiujące cel główny kontroli

Czy w celu świadczenia usług elektronicznych zapewniono sprawne działanie platformy ePUAP oraz podjęto działania na rzecz zwiększenia liczby usług elektronicznych i ich dostępności dla obywateli?

Pytania definiujące cele szczegółowe kontroli

1. Czy Minister Cyfryzacji[5] podejmował skuteczne działania w celu zapewnienia dostępności i zwiększenia liczby e-usług dla obywateli?
2. Czy platforma ePUAP oraz profil zaufany funkcjonują w sposób umożliwiający sprawne i bezpieczne załatwianie spraw przez obywateli i urzędy administracji publicznej?
3. Czy urzędy j.s.t. świadczą e-usługi sprawnie i bezpiecznie?

Jednostki kontrolowane

Kontrolą objęto 30 jednostek: MC, COI i 28 urzędów miast i gmin z obszaru siedmiu województw

Okres objęty kontrolą

Od 1 stycznia 2016 r. do dnia zakończenia kontroli w 2020 r. (5 listopada)

W Polsce stale rośnie liczba osób zainteresowanych załatwianiem spraw urzędowych przez Internet z wykorzystaniem tzw. profilu zaufanego (PZ). Od marca 2019 r. potwierdzanie tożsamości przy załatwianiu spraw przez Internet może nastąpić także z wykorzystaniem nowych dowodów osobistych zawierających warstwę elektroniczną. Wystąpienie pandemii COVID-19 i wprowadzenie szeregu ograniczeń w funkcjonowaniu państwa spowodowało, że w wielu przypadkach cyfrowy kontakt z administracją publiczną był jedynym możliwym. Skutkowało to znaczącym wzrostem liczby spraw załatwianych z wykorzystaniem Elektronicznej Platformy Usług Administracji Publicznej (ePUAP) oraz PZ. Rosnące zainteresowanie e-usługami wpływa na coraz większe obciążenie platformy ePUAP. Dotychczas występowały wielokrotnie sytuacje, gdy była ona mało stabilna lub czasowo niedostępna (problemy z korzystaniem z: miniportalu zamówień publicznych, sprawozdawczości, usługi Twój e-PIT). Zarówno ePUAP, jak i PZ są centralnymi elementami polskiego systemu e-administracji. Zapewnienie ich nieprzerwanego i sprawnego działania jest kluczowe dla prawidłowego funkcjonowania administracji publicznej oraz państwa polskiego w przestrzeni cyfrowej. Dla obywateli ważne jest udostępnienie przez państwo jak największej liczby usług elektronicznych obejmujących swoim zakresem najbardziej istotne sprawy przez nich załatwiane. E-administracja z perspektywy obywatela to intuicyjne i proste formularze interaktywne zasilane danymi będącymi już w posiadaniu administracji publicznej. Jednak jednym z najistotniejszych wyzwań budujących zaufanie obywateli do e-administracji jest zapewnienie bezpieczeństwa wprowadzanych rozwiązań. Jest ono kluczowe mając na względzie jak istotne dane przetwarzane są w związku z załatwianymi przez obywateli sprawami.

Komisja Europejska monitoruje postępy państw członkowskich w zakresie cyfryzacji przy pomocy sprawozdań dotyczących indeksu gospodarki cyfrowej i społeczeństwa cyfrowego (DESI – Digital Economy and Society Index). Sprawozdania te obejmują zarówno profile poszczególnych krajów UE[6], jak i rozdziały tematyczne. W raporcie Komisji Europejskiej z 2020 r. o postępie cyfrowym EU DESI, Polska zajmuje 23 miejsce w UE. W 2019 r. zajmowała 25 miejsce, a w 2018 r. 23 miejsce. W kategorii „Cyfrowe usługi publiczne" Polska w latach 2018–2020 zajmuje miejsce 20.

Kontrola pt. Realizacja usług publicznych dla obywateli z wykorzystaniem platformy ePUAP (P/20/004) została podjęta z inicjatywy własnej Najwyższej Izby Kontroli. W toku kontroli nr P/15/003/KAP Świadczenie usług publicznych w formie elektronicznej na przykładzie wybranych jednostek samorządu terytorialnego ustalono m.in., że pomimo udostępnienia w kontrolowanych urzędach jednostek samorządu terytorialnego różnych e-usług, ich wykorzystanie było niewielkie, a niektóre e-usługi nie były w ogóle wykorzystywane. Liczba udostępnionych e-usług była bardzo

[5] Minister Cyfryzacji kieruje działem administracji rządowej – informatyzacja. Od 6 października 2020 r. jego zadania wykonuje Prezes Rady Ministrów. Zgodnie z rozporządzeniem Prezesa Rady Ministrów z dnia 6 października 2020 r. w sprawie szczegółowego zakresu działania Ministra Cyfryzacji (Dz. U. poz. 1716), jego obsługę zapewnia Kancelaria Prezesa Rady Ministrów.

[6] Coroczne sprawozdania dostępne są na stronie: https://ec.europa.eu/digital-single-market/en/scoreboard/poland.

zróżnicowana pomiędzy badanymi urzędami i kształtowała się od jednej usługi do ponad 100 e-usług. Niewielkie zainteresowanie elektroniczną formą załatwiania spraw wiązało się m.in. z istniejącymi barierami. Część interesantów preferowała osobiste załatwianie sprawy w urzędzie. Kontrolowani jako bariery wskazywali m.in. konieczność dostarczenia do urzędów niektórych dokumentów w postaci papierowej, co powodowało, że niektórych spraw nie można załatwić w formie e-usługi, tj. bez wizyty w urzędzie. Do korzystania z elektronicznej formy załatwiania spraw w urzędach nie zachęcały też stwierdzone wówczas problemy związane z dostępem do e-usług zamieszczonych na ePUAP. Wcześniejsze kontrole wykazały wiele nieprawidłowości w zakresie zapewnienia bezpieczeństwa informacji w urzędach, np. kontrola nr P/18/006 Zarządzanie bezpieczeństwem informacji w jednostkach samorządu terytorialnego.

2. OCENA OGÓLNA

Zapewniono utrzymanie i rozwój ePUAP i PZ oraz zwiększono liczbę e-usług dla obywateli jednak wystąpiły nieprawidłowości w zakresie obliczania dostępności tych systemów

Minister Cyfryzacji w latach 2016–2020 podejmował odpowiednie działania w celu zwiększenia liczby e-usług dla obywateli. Zapewnił także realizację zadań związanych z utrzymaniem i rozwojem platformy ePUAP oraz Profilu Zaufanego. Minister podejmował właściwe działania w celu zwiększenia zainteresowania obywateli profilem zaufanym. W okresie objętym kontrolą trzynastokrotnie wzrosła liczba osób posiadających profil zaufany, co okazało się bardzo istotne w sytuacji epidemii COVID-19 ze względu na możliwość załatwienia części spraw przez Internet. W zarządzaniu systemami ePUAP i PZ wystąpiły jednak nieprawidłowości w obliczaniu ich dostępności, a ponadto MC przed zawarciem aneksu do umowy dotyczącej m.in. utrzymania i rozwoju ePUAP, nie zapewniło niezależnej oceny prawidłowości przygotowanego przez Centralny Ośrodek Informatyki nowego kosztorysu do ww. umowy, mimo że łączne maksymalne wynagrodzenie COI wzrosło o prawie 70 mln zł.

COI na zlecenie MC zapewnił utrzymanie i rozwój systemów ePUAP oraz PZ. Stwierdzono jednak, że zasady obliczania dostępności tych systemów określone w umowach COI z MC były nierzetelne. Raportowana dostępność badanych systemów utrzymywała się powyżej minimalnych progów określonych w umowach, tj. 98% dla ePUAP i 99% dla PZ, co wskazywałoby na ich sprawne działanie, jednakże w raportach tych, zgodnie z umowami, nie uwzględniano wszystkich utrudnień w dostępie użytkowników do systemów, tak więc ocena sprawności systemów wynikająca z raportów nie była w pełni miarodajna. COI podjął odpowiednie działania w celu zmniejszenia powstałych w I połowie 2020 r. zaległości w obsłudze zgłoszeń problemów użytkowników. Ponadto, w COI stwierdzono nieprawidłowości dotyczące:

- **określenia w umowach na utrzymanie systemów ePUAP i PZ zbyt długich maksymalnych czasów obsługi incydentów, co może utrudnić korzystanie z nich przez obywateli i urzędy;**
- **niepełnego wdrożenia Systemu Zarządzania Bezpieczeństwem Informacji (do dnia zakończenia czynności kontrolnych NIK);**
- **przeprowadzenia przez COI niekompletnych testów bezpieczeństwa systemów ePUAP i PZ.**

We wszystkich 28 kontrolowanych urzędach sprawy wpływające w formie elektronicznej za pośrednictwem platformy ePUAP były załatwiane sprawnie, tj. bez zbędnej zwłoki, z wykorzystaniem informacji znajdujących się w urzędzie i danych zgromadzonych w rejestrach publicznych bez zobowiązywania wnioskodawców do dostarczania dodatkowych informacji lub dokumentów będących w posiadaniu urzędu lub innych urzędów. Jednak w 30% badanych urzędów informacje o świadczonych e-usługach były mało czytelne i trudne do odnalezienia na ich stronach internetowych.

W kontrolowanych jednostkach w większości nie zapewniono należytej organizacji bezpieczeństwa informacji, co może stwarzać zagrożenie dla bezpieczeństwa przetwarzania danych i zapewnienia ciągłości pracy urzędu. W szczególności, w 57% badanych urzędów brak było Systemu Zarządzania Bezpieczeństwem Informacji, a w 39% urzędów brakowało pełnej i aktualnej informacji o posiadanych zasobach informatycznych do przetwarzania danych. W 57% z nich nie przeprowadzano obowiązkowych audytów bezpieczeństwa informacji.

3. SYNTEZA WYNIKÓW KONTROLI

Wzrost liczby udostępnionych i zrealizowanych e-usług centralnych

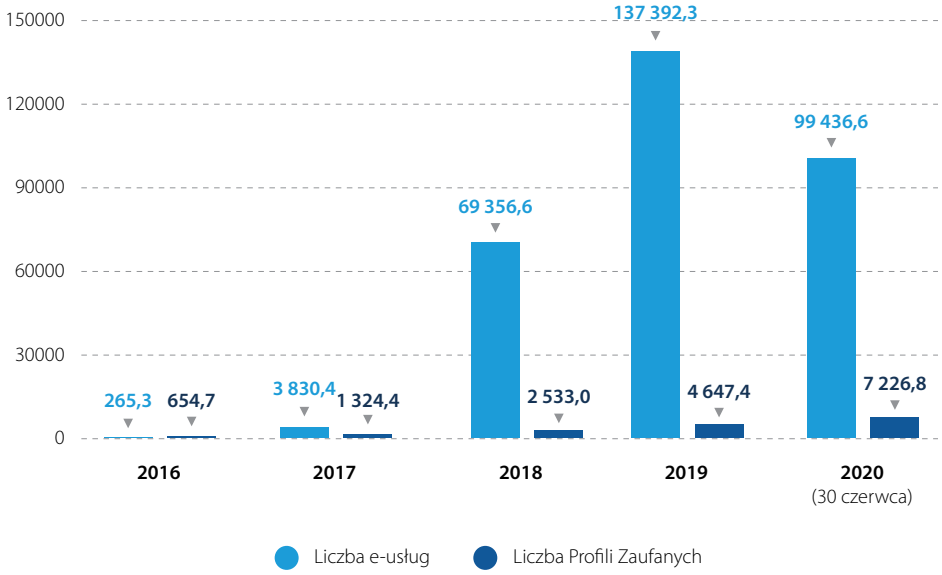
Liczba udostępnionych e-usług centralnych[7] na platformie ePUAP wzrosła w kontrolowanym okresie o 105,6% (z 72 na dzień 1 stycznia 2016 r. do 148 – 30 czerwca 2020 r.). Spośród 148 e-usług centralnych 30 udostępnił Minister Cyfryzacji (wzrost w badanym okresie o 21 usług, tj. o 233,3% w porównaniu do początku roku 2016).

W latach 2016–2020 (do 30 czerwca) nastąpił wzrost liczby spraw zrealizowanych w formie e-usług. Zrealizowano łącznie 310 284,2 tys. e-usług, z tego w: 2016 r. – 265,3 tys., 2017 r. – 3830,4 tys., 2018 r. – 69 356,6 tys., 2019 r. – 137 392,3 tys., do 30 czerwca 2020 r. – 99 439,6 tys. [str. 16–19]

Wzrost liczby obywateli posiadających profil zaufany

W okresie objętym kontrolą nastąpił ponad trzynastokrotny wzrost liczby obywateli posiadających profil zaufany (z 524,3 tys. na 1 stycznia 2016 r. do 7226,8 tys. na 30 czerwca 2020 r.[8]). Ponadto następował systematyczny wzrost wykorzystywania profilu zaufanego przez obywateli w kontaktach z administracją. W kwietniu 2020 r., w związku z epidemią COVID-19, MC uruchomiło możliwość założenia przez obywateli tymczasowego profilu zaufanego, którego ważność wynosiła trzy miesiące. Do 30 czerwca 2020 r. założono 12,0 tys. tymczasowych profili zaufanych. [str. 19–22]

Infografika nr 1
Liczba e-usług zrealizowanych poprzez ePUAPoraz liczba profili zaufanych w latach 2016–2020 (w tys.)



Źródło: opracowanie własne NIK na podstawie danych z kontroli.

Brak niezależnej oceny kalkulacji zwiększających koszty związane z utrzymaniem ePUAP i PZ przez COI

Usługi w zakresie zapewnienia poprawnego i nieprzerwanego funkcjonowania ePUAP realizowane były przez COI na podstawie umowy zawartej z MC 4 kwietnia 2016 r. W latach 2016–2017 umowa ta obejmowała także utrzymanie systemu Profil Zaufany. Aneksem nr 4 z dnia 4 kwietnia 2019 r.

[7] Tj. e-usługi udostępnione przez centralne ograny administracji państwowej obowiązujące na terenie całego kraju.

[8] Według danych na stronie https://www.gov.pl/web/cyfryzacja/e-uslugowe-podsumowanie-2020-r , liczba osób posiadających profil zaufany 31 grudnia 2020 r. wynosiła 8 816,6 tys.

do ww. umowy łączne maksymalne wynagrodzenie dla COI zwiększono do kwoty 106 687,2 tys. zł netto, tj. o 69 857,9 tys. zł (o 189,7%) w porównaniu do pierwotnej umowy. Zwiększenie wynagrodzenia wynikało w szczególności: z wydłużenia okresu obowiązywania umowy o kolejne 36 miesięcy, dodania kolejnego systemu obejmującego 18 e-usług, wzrostu kosztów utrzymania i usług dodatkowych. **Ministerstwo Cyfryzacji nie zapewniło niezależnej oceny sporządzonych przez COI kalkulacji zwiększających koszty umowy ePUAP, skutkujących zwiększeniem wynagrodzenia wykonawcy, a także nie udokumentowało procesu negocjacji wynagrodzenia COI.** [str. 22–24]

Realizacja zadań MC określonych w SOR

Minister Cyfryzacji należycie realizował cel określony w *Strategii na rzecz Odpowiedzialnego Rozwoju do roku 2020 (z perspektywą do 2030 r.),* tj. *stworzenie cyfrowego państwa usługowego poprzez udostępnienie wysokiej jakości usług na rzecz obywateli, w tym również przedsiębiorców.* Wskaźnik realizacji ww. celu, odnoszący się do procentu liczby osób korzystających z Internetu w kontaktach z administracją publiczną, na koniec 2019 r. wyniósł 31,4% (zaplanowana w SOR wartość na koniec 2020 r. to 32,0%) [str. 26–36]

Zapewnienie sprawnego działania ePUAP oraz PZ

W umowach MC z COI na utrzymanie systemów ePUAP i PZ dostępność SLA[9] określono na poziomie 98% w odniesieniu do systemu ePUAP oraz 99% w odniesieniu do systemu PZ. Przyjęcie takich wartości oznacza dopuszczenie możliwości zaistnienia całkowitej niedostępności każdej z usług przez 7,3 dnia w ciągu roku dla systemu ePUAP oraz przez 3,6 dnia dla systemu PZ. Określony w umowach na utrzymanie systemów ePUAP i PZ, i stosowany w przekazywanych przez COI do MC raportach sposób obliczania dostępności tych systemów nie uwzględnia ich rzeczywistej dostępności, która dla użytkowników była faktycznie niższa niż raportowana dostępność na poziomie 100%. Kontrola wykazała bowiem, że zgodnie z umowami na utrzymanie systemów raportowany czas ich dostępności może zmniejszyć jedynie zaistnienie incydentu krytycznego. Przyjęcie w umowach wąskiej definicji incydentu krytycznego powoduje, że awaria uzasadniająca sklasyfikowanie incydentu jako krytycznego jest w praktyce trudna do zaistnienia. Z ustaleń kontroli wynika, że miały miejsce incydenty, które powodowały brak możliwości skorzystania z ww. systemów przez użytkowników, a które zgodnie z definicją przyjętą w umowach nie były klasyfikowane jako incydenty krytyczne i zatem nie wpływały na obniżenie raportowanego poziomu dostępności. W umowach na utrzymanie systemów ePUAP i PZ ustalono maksymalne czasy obsługi poszczególnych kategorii zgłoszeń, które są zbyt długie (10 dni dla incydentów pilnych i 20 dni dla incydentów standardowych), gdyż mogą utrudnić korzystanie z tych systemów przez obywateli i urzędy.

Z perspektywy obywatela oraz przedsiębiorcy istotne jest aby mógł załatwić sprawę drogą elektroniczną szybko i sprawnie. NIK po przeprowadzonej w 2015 r. kontroli nr P/15/003/KAP *Świadczenie usług publicznych w formie elektronicznej* wskazywała, że do korzystania z elektronicznej formy zała-

[9] SLA – umowa o poziomie świadczenia usług informatycznych i ich parametrach (ang. *Service Level Agreement*).

twiania spraw w urzędach nie zachęcały problemy związane z niezadowalającą dostępnością e-usług zamieszczonych na platformie ePUAP, co istotnie utrudniało obywatelom korzystanie z tych usług. Z ustaleń obecnej kontroli nr P/20/004/KAP *Realizacja usług publicznych dla obywateli z wykorzystaniem platformy ePUAP* wynika, że zgłaszane przez użytkowników problemy z dostępem do profilu zaufanego i do usług zamieszczonych na platformie ePUAP nie zawsze były szybko rozwiązywane. Wskazane byłoby zatem dalsze zwiększenie poziomu dostępności systemów PZ oraz ePUAP oraz działania na rzecz skrócenia czasu rozwiązywania zgłaszanych problemów, co jest szczególnie istotne w przypadku profilu zaufanego, gdyż uwierzytelnienie się osoby za jego pośrednictwem warunkuje możliwość skorzystania z elektronicznych usług administracji publicznej. NIK zauważa, że zapewnienie prawidłowego funkcjonowania systemów ePUAP i PZ zależy od współpracy pomiędzy Ministrem Cyfryzacji i COI. [str. 40–43]

Wsparcie techniczne dla użytkowników ePUAP i PZ

Wsparcie techniczne dla użytkowników tych systemów zostało zorganizowane zgodnie ze współczesną praktyką w tym zakresie. **COI przyjęło nierzetelny mechanizm pomiaru jakości obsługi zgłoszeń. Dane zaprezentowane w raportach utrzymania systemów ePUAP i PZ, dotyczące skuteczności obsługi zgłoszeń przez COI w danym miesiącu nie odzwierciedlały rzeczywistości.** Pomimo, iż np. w marcu 2020 r. obsługa odpowiednio 76% incydentów dotyczących PZ i 63% incydentów dotyczących ePUAP nie została nawet otwarta, zaraportowana do MC skuteczność obsługi zgłoszeń dla ePUAP wynosiła w marcu 93,6%, a w kwietniu 96,9%, natomiast dla PZ wyniosła odpowiednio 96,2% i 95,9%.

Umowy na utrzymanie systemów ePUAP i PZ, wbrew praktyce rynkowej nie określają wymaganych czasów reakcji na zgłoszenie, tj. czasu, jaki może upłynąć od zarejestrowania zgłoszenia w systemie do rozpoczęcia jego obsługi. [str. 43–45]

Zaległości w obsłudze zgłoszeń problemów przez COI w I połowie 2020 r.

Zaległości w obsłudze zgłoszeń wpływających od użytkowników tych systemów narastały w I połowie 2020 r., co spowodowane było zwiększonym wykorzystaniem tych platform przez obywateli i urzędy w związku ze stanem epidemii COVID-19. W COI podjęto odpowiednie działania zmierzające do poprawy tej sytuacji. [str. 45–46]

Monitorowanie działania ePUAP i PZ

COI skutecznie monitorował działanie systemów ePUAP i PZ, reagując na pojawiające się awarie. Monitorowanie działania systemów ePUAP i PZ realizowane jest w trybie 24 godziny na dobę, przez siedem dni w tygodniu. Wykorzystywane są w tym celu specjalistyczne narzędzia, które służą do bieżącego monitorowania zajętości infrastruktury systemów ePAUP i PZ. [str. 46–47]

Rozwój systemów ePUAP i PZ

COI na zlecenie Ministerstwa Cyfryzacji rozwijał systemy ePUAP i PZ, i podjął w tym zakresie współpracę z interesariuszami. Prace rozwojowe systemu ePUAP dotyczyły m.in. realizacji nowych e-usług, integracji ePUAP z innymi systemami i rejestrami. Rozwój PZ dotyczył m.in. stworzenia podpisu eDowodu oraz automatycznej aktualizacji danych na podstawie zmian w rejestrze PESEL. Realizowany przez COI proces zarządzania zmianami od strony proceduralno-zarządczej był zorganizowany prawidłowo, w sposób typowy dla tego rodzaju procesów. [str. 47–49]

Zapewnienie bezpieczeństwa systemów ePUAP i PZ

W COI podjęto działania w celu wdrożenia wymagań międzynarodowej normy z zakresu bezpieczeństwa informacji ISO/IEC 27001. Do dnia zakończenia czynności kontrolnych nie w pełni wdrożono System Zarządzania Bezpieczeństwem Informacji. COI nie przeprowadził właściwych, kompletnych testów penetracyjnych systemów ePUAP i PZ, co było działaniem nierzetelnym. Przeprowadzenie pełnych testów jest niezbędne dla uzyskania potwierdzenia, że systemy ePUAP i PZ, które są użytkowane przez obywateli oraz urzędy, są bezpieczne. W odpowiedzi na wystąpienie pokontrolne COI poinformował, że podejmie niezwłoczne działania w tym zakresie, m.in. dotyczące przeprowadzenia właściwych testów systemów ePUAP i PZ. [str. 49–52]

Zapewnienie ciągłości działania systemów ePUAP i PZ

COI przygotował oraz wdrożył odpowiednie rozwiązania techniczne i organizacyjne dla ePUAP i PZ w celu zapewnienia ciągłości działania w sytuacji wystąpienia znaczącej awarii lub katastrofy. [str. 53–54]

Uwzględnienie w strategiach j.s.t. załatwiania spraw drogą elektroniczną

Większość kontrolowanych urzędów miast oraz gmin (68%) uwzględniła w swoich dokumentach strategicznych zagadnienia dotyczące ich dostosowania do elektronicznego świadczenia usług publicznych. [str. 55–56]

Liczba udostępnionych i zrealizowanych usług elektronicznych w kontrolowanych urzędach

We wszystkich objętych badaniem urzędach udostępniano od 10 do 232 usług elektronicznych z wykorzystaniem platformy ePUAP. NIK zauważa, że świadczenie przez urzędy j.s.t. usług w formie elektronicznej, poza wyjątkami wynikającymi z ustaw, nie jest obligatoryjne, stąd różne mogą być liczby e-usług udostępnianych przez poszczególne urzędy. Zdaniem NIK, należy jednak dążyć do zwiększenia liczby udostępnianych e-usług, biorąc pod uwagę sprawy najczęściej załatwiane przez obywateli. Według stanu na dzień 31 maja 2020 r. skontrolowane urzędy[10] na platformie ePUAP udostępniały łącznie 1402 usługi elektroniczne. W ośmiu urzędach (tj. w 29%) obywatele mogli skorzystać z ponad 50 usług za pośrednictwem platformy ePUAP. Najwięcej e-usług udostępniono w zakresie spraw obywatelskich (dowody osobiste, meldunki, wybory), a także spraw dotyczących budownictwa, architektury, urbanistyki, podatków i opłat oraz nieruchomości, lokali mieszkalnych i użytkowych i ochrony środowiska.

Liczba e-usług zrealizowanych przez obywateli w kontrolowanych urzędach w okresie od 1 stycznia 2020 r. do 30 czerwca 2020 r. wyniosła łącznie 30 580 e-usług. Najczęściej korzystano z e-usług w zakresie złożenia pisma ogólnego, spraw obywatelskich (akty stanu cywilnego, dowody osobiste, meldunki, wybory), wniesienia skargi oraz zapytania do urzędu (ESP). [str. 56–58]

Wzrost zainteresowania e-usługami w okresie epidemii COVID-19

We wszystkich kontrolowanych urzędach w okresie od 1 marca do 30 czerwca 2020 r., tj. w początkowym okresie epidemii COVID-19 w Polsce nastąpił znaczny, niekiedy ponad dwukrotny wzrost zainteresowania e-usługami. [str. 56–58]

[10] UM w Łomży stan na 30 czerwca 2020 r., UM w: Legionowie i Zgorzelcu stan na 15 lipca 2020 r., UM w Oleśnicy stan na 11 sierpnia 2020 r.

Dokumentowanie przebiegu i rozstrzygania spraw w urzędach

Spośród 28 kontrolowanych urzędów, w 96% z nich podstawowym sposobem dokumentowania przebiegu i rozstrzygania spraw był system tradycyjny (papierowy) wspomagany przez systemy elektronicznego obiegu dokumentów. W jednym urzędzie był to system elektroniczny. [str. 58–59]

Realizowanie spraw z zakresu usług elektronicznych, wpływających do urzędów poprzez ePUAP

Dekretacja dokumentów elektronicznych (od momentu wpływu/rejestracji wniosku/formularza) następowała na ogół niezwłocznie. Tylko w nielicznych przypadkach dekretacja sprawy do załatwienia przez pracownika następowała po upływie kilkunastu dni.

W 75% urzędów część analizowanych wniosków/formularzy od obywateli wymagało korekt i uzupełnień, przy czym **w żadnym z kontrolowanych urzędów nie wymagano osobistego stawiennictwa obywatela w celu uzupełnienia wniosku**. **Przy załatwianiu spraw pracownicy wszystkich kontrolowanych urzędów korzystali z danych gromadzonych w zewnętrznych systemach i rejestrach państwowych** takich jak np. PESEL, Rejestr Dowodów Osobistych, Elektroniczne Księgi Wieczyste, Baza Usług Aktów Stanu Cywilnego, Ewidencja Gruntów i Budynków.

We wszystkich kontrolowanych urzędach możliwe było uzyskanie informacji na temat aktualnego stanu załatwianej sprawy, np. mailem, przez stronę BIP lub poprzez ePUAP. [str. 59–60]

Działania informacyjne urzędów w zakresie e-usług

W 96% kontrolowanych urzędów podejmowano działania w celu informowania obywateli o możliwości załatwienia spraw drogą elektroniczną. Jednak w 33% z nich informacje te były niekompletne, mało czytelne i trudne do odnalezienia na stronach internetowych urzędów. [str. 62–63]

Szkolenia w zakresie bezpieczeństwa informacji

W 82% kontrolowanych urzędów, zgodnie z § 20 ust. 2 pkt 6 rozporządzenia KRI zorganizowano szkolenia dla pracowników zaangażowanych w proces przetwarzania informacji **z zakresu komunikacji elektronicznej oraz zagrożeń z tym związanych, a także dotyczących bezpieczeństwa informacji.** W urzędach, w których nie zapewniono pełnych szkoleń pracowników w zakresie bezpieczeństwa informacji, szkolenia dotyczyły wyłącznie obsługi wdrożonych programów wspomagających procedurę obiegu dokumentów lub ochrony danych osobowych. [str. 63–64]

Brak procedur w zakresie bezpieczeństwa informacji

W 57% objętych kontrolą urzędów brak było Systemu Zarządzania Bezpieczeństwem Informacji, o którym mowa w § 20 ust. 1 w związku z ust. 3 rozporządzenia KRI. W szczególności w urzędach tych nie ustanowiono polityk bezpieczeństwa informacji. Opracowane i wdrożone w tych jednostkach regulacje dotyczyły głównie ochrony danych osobowych i nie obejmowały bezpieczeństwa innych informacji.

NIK zauważa, że w większości skontrolowanych urzędów j.s.t. nie zapewniono właściwej organizacji bezpieczeństwa informacji, co może stwarzać zagrożenie dla bezpieczeństwa przetwarzania danych i zapewnienia ciągłości pracy tych urzędów. Na nieprawidłowości i zaniechania w zakresie zapewnienia bezpieczeństwa informacji w urzędach miast i gmin NIK wskazywała już we wcześniejszych kontrolach. W szczególności, w wyniku przeprowadzonej w 2016 r. kontroli nr P/16/006/KAP dotyczącej funkcjonowania Systemu Rejestrów Państwowych stwierdzono, że w 62% kon-

trolowanych urzędów miast brak było kompletnych procedur w zakresie bezpieczeństwa informacji. W 2017 r. po kontroli nr P/17/062/LBI *Bezpieczeństwo elektronicznych zasobów informatycznych w j.s.t. w województwie podlaskim* NIK oceniła, że w prawie wszystkich skontrolowanych jednostkach poziom bezpieczeństwa systemów informatycznych i usług sieciowych był na niezadowalającym lub na bardzo niskim poziomie. Po przeprowadzeniu w 2018 r. kontroli nr P/18/006/KAP *Zarządzanie bezpieczeństwem informacji w jednostkach samorządu terytorialnego*, NIK w blisko 70% skontrolowanych urzędów j.s.t. negatywnie oceniła wykonywanie zadań związanych z zapewnieniem bezpieczeństwa przetwarzania informacji. Ustalenia obecnej kontroli nr P/20/004/KAP *Realizacja usług publicznych dla obywateli z wykorzystaniem platformy ePUAP* wskazują, że pomimo upływu czasu sytuacja w tym zakresie nie uległa zasadniczej poprawie, zatem zapewnienie bezpieczeństwa przetwarzanych danych wymaga podjęcia przez urzędy j.s.t. szeregu działań zarówno organizacyjnych, jak i technicznych. Jest to szczególnie istotne nie tylko ze względu na wymagania wynikające z rozporządzenia KRI oraz RODO, ale także z tego względu, że coraz więcej danych obywateli jest przetwarzanych w systemach informatycznych i coraz więcej spraw załatwianych jest przez obywateli w urzędach drogą elektroniczną. [str. 64–65]

Niewłaściwe zarządzanie uprawnieniami użytkowników systemów informatycznych

W 32% urzędów, 59 byłych pracowników posiadało aktywne konta w systemach informatycznych, gdyż nie zostały one zablokowane, co było niezgodne z § 20 ust. 2 pkt 5 rozporządzenia KRI.

W 18% urzędów część użytkowników, a w jednym urzędzie wszyscy kontrolowani użytkownicy, posiadali na swoich komputerach uprawnienia administratora systemu, w związku z tym mieli możliwość zainstalowania dowolnego oprogramowania, co było niezgodne z § 20 ust. 2 pkt 4 rozporządzenia KRI. [str. 65–67]

Nieprzeprowadzanie audytów bezpieczeństwa informacji

W 57% urzędów w okresie objętym kontrolą nie przeprowadzano audytu w zakresie bezpieczeństwa informacji, co było niezgodne z § 20 ust. 2 pkt 14 rozporządzenia KRI. [str. 66–67]

Brak informacji lub niepełna informacja o posiadanych zasobach informatycznych

W 39% urzędów brak było aktualnych informacji o posiadanym sprzęcie i oprogramowaniu służącym do przetwarzania informacji obejmującej ich rodzaj i konfigurację, co było niezgodne z § 20 ust. 2 pkt 2 rozporządzenia KRI. W siedmiu z tych urzędów (64%), w których wykorzystywano oprogramowanie do ewidencjonowania sprzętu i oprogramowania wraz z ich konfiguracją, dane w nim zawarte były nierzetelne. W czterech urzędach (36%) spis urządzeń informatycznych prowadzono w formie arkusza danych lub wykazów papierowych, co nie gwarantowało aktualności informacji. [str. 65]

4. WNIOSKI

Po kontroli NIK wnioskuje aby:

Minister Cyfryzacji[11]

1. Dokonać zmiany sposobu obliczania dostępności systemów ePUAP i PZ poprzez uwzględnienie czasu trwania incydentów, które wpływają na faktyczny brak możliwości korzystania z tych systemów zgodnie z ich przeznaczeniem, bez względu na ich sklasyfikowanie jako standardowe, pilne, czy krytyczne.
2. Dokonać zmiany definicji incydentu krytycznego dla systemów ePUAP i PZ w ten sposób, aby uwzględniała ona brak możliwości lub istotne ograniczenie w korzystaniu z którejkolwiek z głównych funkcji tych systemów.
3. W przypadku realizacji projektów informatycznych zapewnić rzetelną weryfikację kalkulacji kosztów, przedstawionej przez kontrahenta, przez niezależnych ekspertów własnych lub zewnętrznych posiadających kompetencje w zakresie wyceny projektów informatycznych oraz zapewnienie rzetelnego dokumentowania procesu negocjacji kosztów wynagrodzenia dla wykonawców.

Dyrektor Centralnego Ośrodka Informatyki

1. Uwzględniać w obliczanej dostępności systemów ePUAP i PZ także incydenty niezamknięte w danym miesiącu.
2. Skrócić gwarantowane czasy obsługi incydentów pilnych i standardowych dotyczących ePUAP oraz PZ.
3. Określić czas reakcji na zgłoszenie dotyczące ePUAP i PZ, tj. czas, jaki może upłynąć od zarejestrowania zgłoszenia w systemie do rozpoczęcia jego obsługi.
4. Wprowadzić zmiany w zakresie sposobu raportowania o obsłudze zgłoszeń od użytkowników ePUAP i PZ gdzie będzie uwzględniany nie tylko sam fakt przekroczenia terminu na obsługę zgłoszeń, ale również długość okresu tej obsługi.

Prezydenci miast, burmistrzowie i wójtowie

W opinii NIK, konieczne jest aby kierownicy urzędów jednostek samorządu terytorialnego zwrócili uwagę na zapewnienie bezpieczeństwa informacji w urzędach, w szczególności na:

1. Opracowanie i wdrożenie systemu zarządzania bezpieczeństwem informacji, a w szczególności polityki bezpieczeństwa informacji.
2. Prowadzenie i bieżące aktualizowanie ewidencji posiadanych zasobów informatycznych wraz z ich konfiguracją.
3. Zapewnienie niezwłocznego blokowania dostępu i odbierania uprawnień do systemów informatycznych pracownikom, którzy zakończyli zatrudnienie w urzędzie.
4. Zapewnienie przynajmniej raz w roku okresowego audytu bezpieczeństwa informacji.

[11] Zgodnie z rozporządzeniem Prezesa Rady Ministrów z dnia 6 października 2020 r. w sprawie szczegółowego zakresu działania Ministra Cyfryzacji (Dz. U. poz. 1716), minister kieruje działem administracji rządowej – informatyzacja, a jego obsługę zapewnia Kancelaria Prezesa Rady Ministrów. Zadania Ministra Cyfryzacji wykonuje odtąd Prezes Rady Ministrów.

5. WAŻNIEJSZE WYNIKI KONTROLI

5.1. Realizacja przez Ministra Cyfryzacji działań w celu zapewnienia dostępności i zwiększenia liczby e-usług dla obywateli

Minister Cyfryzacji podejmował działania w celu zapewnienia dostępności i zwiększenia liczby e-usług dla obywateli

Minister Cyfryzacji w latach 2016–2020 podejmował odpowiednie działania w celu zapewnienia dostępności i zwiększenia liczby e-usług dla obywateli. Zgodnie z art. 19a ust. 1 ustawy o informatyzacji zapewniał funkcjonowanie platformy ePUAP, na której udostępniane były e-usługi centralne. Liczba udostępnionych e-usług centralnych na tej platformie wzrosła w kontrolowanym okresie o 105,6% (z 72 na dzień 1 stycznia 2016 r. do 148 na dzień 30 czerwca 2020 r.). Spośród 148 e-usług centralnych, 30 udostępnił Minister Cyfryzacji (wzrost w badanym okresie o 21 usług, tj. o 233,3% w porównaniu do początku roku 2016). Przed uruchomieniem nowych e-usług Minister przeprowadził badanie, którego celem było określenie potrzeb i postaw obywateli wobec załatwiania spraw urzędowych drogą elektroniczną.

W okresie objętym kontrolą Minister Cyfryzacji realizował cel określony w *Strategii na rzecz Odpowiedzialnego Rozwoju do roku 2020 (z perspektywą do 2030 r.),* tj. *stworzenie cyfrowego państwa usługowego poprzez udostępnienie wysokiej jakości usługi na rzecz obywateli, w tym również przedsiębiorców.* Działania te skutkowały wzrostem wskaźnika określonego dla ww. celu, odnoszącego się do liczby osób korzystających z Internetu w kontaktach z administracją publiczną. Na koniec 2019 r. wartość tego wskaźnika wyniosła 31,4% (zaplanowana w SOR wartość wskaźnika w roku 2020 to 32,0%).

Minister Cyfryzacji zapewnił realizację zadań związanych z utrzymaniem i rozwojem platformy ePUAP i Profilu Zaufanego. Jednak w zawartej przez MC umowie ePUAP i umowie PZ, dotyczącej utrzymania tych systemów przez COI, ustalono zbyt długie maksymalne czasy obsługi poszczególnych kategorii incydentów, co w konsekwencji wydłużało proces usuwania problemów zgłaszanych przez użytkowników.

Minister podejmował właściwe działania organizacyjne i informacyjno-promocyjne w celu zwiększenie zainteresowania profilem zaufanym wśród obywateli. W okresie objętym kontrolą ponad trzynastokrotnie wzrosła liczba obywateli posiadających profil zaufany. Według stanu na 1 stycznia 2016 r. obywatele posiadali 524,3 tys. profili zaufanych, na koniec czerwca 2020 r. było ich 7226,8 tys. Systematycznie wzrastało również wykorzystywanie profilu zaufanego przez obywateli w kontaktach z administracją z 1908,0 tys. w 2016 r. do 20 869,8 tys. tylko w pierwszej połowie roku 2020.

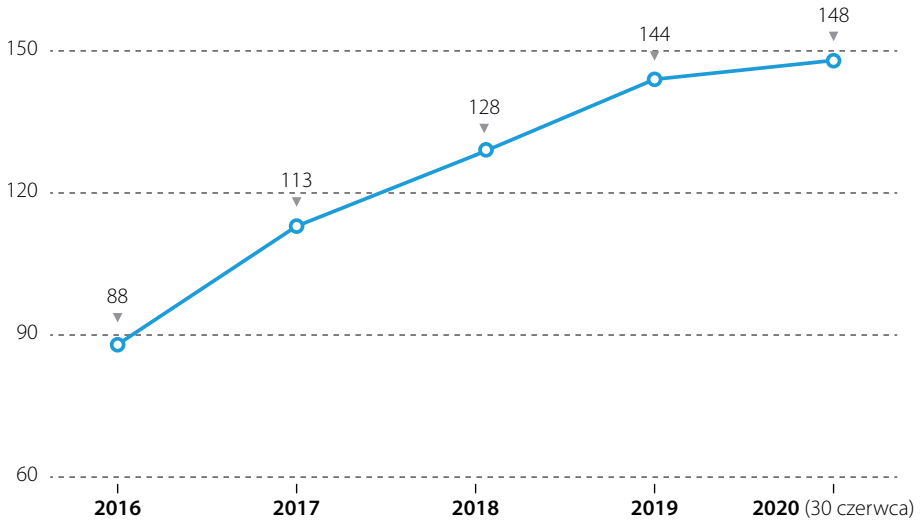
Stwierdzona nieprawidłowość dotyczyła niezapewnienia przez MC przed zawarciem aneksu nr 4 do umowy dotyczącej m.in. utrzymania i rozwoju ePUAP, niezależnej oceny prawidłowości przygotowanego przez Centralny Ośrodek Informatyki nowego kosztorysu do ww. umowy oraz nieudokumentowania procesu negocjacji kosztów wynagrodzenia dla COI.

Liczba e-usług centralnych udostępnionych obywatelom przez Ministra Cyfryzacji

W ramach systemu ePUAP na dzień 1 stycznia 2016 r. funkcjonowały 72 e-usługi centralne[12]. W każdym kolejnym roku objętym kontrolą zwiększała się liczba e-usług udostępnionych na ePUAP. I tak:

- na koniec 2016 r. udostępniano 88 e-usług (ich liczba w ciągu roku zwiększyła się o 16, tj. o 22,2%);
- na koniec 2017 r. udostępniano 113 e-usług (wzrost o 25, tj. o 28,4% w stosunku do 2016 r.);
- na koniec 2018 r. udostępniano 128 e-usług (zwiększenie o 15, tj. o 13,3% w stosunku do 2017 r.);
- na koniec 2019 r. udostępnione były 144 e-usługi (wzrost o 16, tj. o 12,5% w stosunku do 2018 r.);
- na dzień 30 czerwca 2020 r. udostępnionych było łącznie 148 e-usług (wzrost o cztery e-usługi, tj. o 2,8% w porównaniu do końca 2019 r.).

Infografika nr 2
Liczba e-usług centralnych udostępnionych na ePUAP w latach 2016–2020



Źródło: opracowanie własne NIK na podstawie danych z kontroli.

Minister Cyfryzacji pełnił rolę podmiotu udostępniającego e-usługi w przypadku 30 e-usług centralnych, tj. 20,3% spośród wszystkich 148 udostępnionych na platformie ePUAP. W okresie od stycznia 2016 r. do 30 czerwca 2020 r. Minister udostępnił łącznie 21 e-usług (wzrost o 233,3%, w stosunku do ośmiu usług udostępnionych na koniec 2015 r.).

Podstawą określenia zapotrzebowania społecznego w zakresie e-usług był raport z przeprowadzonego w 2016 r. badania pn. „E-administracja w oczach internautów”[13], którego celem było między innymi określenie potrzeb i postaw obywateli wobec załatwiania spraw urzędowych drogą elektroniczną. W raporcie tym wskazano, że dla 61,0% badanych najważ-

[12] Tj. e-usługi udostępnione przez centralne ograny administracji państwowej, świadczone na terenie całego kraju.

[13] Badanie przeprowadzone zostało w czerwcu 2016 r. przez agencję badawczą PBS, na grupie 4801 osób. Raport udostępniony na stronie: https://www.gov.pl/web/cyfryzacja/e-administracja-w-oczach-internautow-raport-z-badania-2016.

niejszym rodzajem spraw, które chcieliby załatwić przez Internet było wydanie/wymiana dokumentów (dowód osobisty, paszport, prawo jazdy), dla 51,0% były to sprawy związane ze zdrowiem (zapisy do lekarza, konsultacje online, recepta elektroniczna), a dla 45,0% sprawy związane z rejestracją pojazdu (rejestracja, wyrejestrowanie, zgłoszenie sprzedaży, wydanie wtórników np. tablic rejestracyjnych, karty pojazdu, znaków legalizacyjnych, nalepki kontrolnej. Ponadto 79,8% badanych wskazało, że chciałoby otrzymywać od administracji publicznej powiadomienia o upływie terminu ważności dokumentu, a 69,9% powiadomienia o dokumencie gotowym do odbioru.

W latach 2017–2020 (do 30 czerwca) Ministerstwo Cyfryzacji nie przeprowadzało innych badań dotyczących zapotrzebowania na e-usługi.

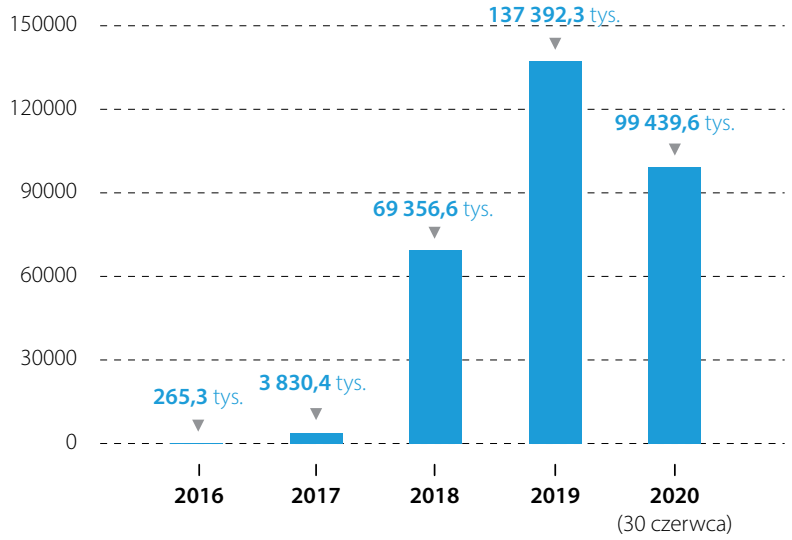
Dyrektor Generalny MC wyjaśnił, że wyniki badania z 2016 r. oraz bieżące potrzeby wynikające ze zmian legislacyjnych definiowały zakres prac w ramach planu pracy Ministra Cyfryzacji. Stwierdził, że w pierwszej kolejności wdrażano usługi, które zgodnie z badaniem z 2016 r. generowały największe zainteresowanie użytkowników, a także usługi wynikające z zaplanowanych w MC projektów, np. Rozwój Systemu Rejestrów Państwowych lub „e-Dowód 2.0". Dodał, że usługi były także uruchamiane na podstawie zapotrzebowania zgłaszanego przez inne resorty w związku ze zmianami legislacyjnymi.

Ponadto w MC dokonywano analizy wniosków i skarg obywateli dotyczących działania systemu ePUAP i e-usług. W okresie objętym kontrolą wpłynęło do MC 116 takich skarg i 24 wnioski. Skargi dotyczyły głównie nieprawidłowości w funkcjonowaniu systemu ePUAP, w szczególności braku dostępności systemu, braku doręczenia pisma (korespondencji) pomimo otrzymania UPO[14], braku kontaktu z telefoniczną obsługą klienta, sposobu wyszukiwania informacji w ePUAP, braku intuicyjności sytemu, braku możliwości otwarcia korespondencji, czy wysyłania kodów autoryzacyjnych tylko na telefon komórkowy, co wyklucza osoby nieposiadające telefonów komórkowych. MC uznało, że 31 skarg było zasadnych, 16 częściowo zasadnych, 69 niezasadnych. Dziewięć wniosków zostało uwzględnionych, a 15 nie uwzględniono.

Za pośrednictwem ePUAP w latach 2016–2020 (do 30 czerwca) zrealizowano łącznie 310 284,2 tys. e-usług, z tego w: 2016 r. – 265,3 tys., 2017 r. – 3830,4 tys., 2018 r. – 69 356,6 tys., 2019 r. – 137 392,3 tys., do 30 czerwca 2020 r. – 99 439,6 tys.

[14] Urzędowe Poświadczenie Odbioru.

Infografika nr 3
Liczba e-usług zrealizowanych poprzez ePUAP w latach 2016–2020 (w tys.)



Źródło: opracowanie własne NIK na podstawie danych z kontroli.

Wśród udostępnionych e-usług przez ePUAP, obywatele najczęściej korzystali z e-usługi pn. „Sprawdź historię pojazdu" (usługa udostępniona przez Ministra Cyfryzacji). Od jej uruchomienia w 2018 r. do 30 czerwca 2020 r. z usługi tej skorzystano 285 900,7 tys. razy. W okresie objętym kontrolą usługa ta stanowiła 92,1% wszystkich zrealizowanych e-usług. W ramach kolejnych 12 najpopularniejszych wśród użytkowników e-usług wygenerowano łącznie 22 540,6 tys. wniosków[15]. Łącznie 13 najpopularniejszych e-usług, w tym 12 udostępnionych przez Ministra Cyfryzacji, odpowiadało za 99,4% wniosków złożonych za pośrednictwem platformy ePUAP. W przypadku 68 usług centralnych udostępnionych na platformie ePUAP (tj. 45,9% wszystkich udostępnionych e-usług) żadna nie została wykorzystana w całym okresie objętym kontrolą (4,5 roku kalendarzowego) więcej niż 100 razy. Wśród nich 19, tj. 12,8% wszystkich e-usług, nie zostało wykorzystane w ww. okresie ani razu, np. *Rekompensata utraconych dochodów gmin, Przekazanie materiałów archiwalnych do właściwego archiwum państwowego, Wydanie zgody na brakowanie dokumentacji niearchiwalnej*.

Dyrektor Generalny MC wskazał, że podmiotami właściwymi do udzielenia informacji w zakresie przesłanek uruchomienia e-usług, które nie były wykorzystywane lub ich wykorzystanie było znikome, są podmioty udostępniające te usługi. Wyjaśnił, że *zgodnie z art. 19a ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne, minister właściwy do spraw informatyzacji zapewnia funkcjonowanie platformy ePUAP. (...) Podmioty udostępniające usługi*

[15] Pismo ogólne – stary wzór – 9673,5 tys.; Podpisz dokument elektronicznie (Podpisywarka) – 2717,5 tys.; Sprawdź swój pojazd – 1854,4 tys.; Pismo ogólne do podmiotu publicznego – 1388,2 tys.; Sprawdź swoje punkty karne – 1159,2 tys.; Sprawdź swoje dane w Rejestrze Dowodów Osobistych – 988,0 tys.; Wydanie karty EKUZ w związku z pobytem czasowym za granicą – 982,9 tys.; Sprawdź swoje dane w rejestrze PESEL – 865,2 tys.; Dopisz się do spisu wyborców – 841,3 tys.; Wniosek o wydanie dowodu osobistego – 773,6 tys.; Podpisz JPK_VAT GOV – 672,6 tys.; Zawiadomienie o zbyciu lub nabyciu pojazdu – 624,2 tys.

na ePUAP zapewniają ich zgodność z przepisami stanowiącymi podstawę sporządzenia wzoru dokumentu elektronicznego oraz dokonują aktualizacji tych usług w katalogu usług.

W grupie usług o najniższym zainteresowaniu obywateli znajdowała się jedna e-usługa udostępniona przez Ministra Cyfryzacji pn. „Przekazanie informacji o udostępnionym przez podmiot publiczny adresie Elektronicznej Skrzynki Podawczej" udostępniona w 2015 r. i wykorzystana jedynie 12 razy.

Dyrektor Generalny MC poinformował, że *usługa ta została uruchomiona w 2015 r. w celu umożliwienia podmiotom publicznym wywiązanie się z wynikającego z art. 16 ust. 1b ustawy o informatyzacji, obowiązku informowania Ministra właściwego do spraw informatyzacji o adresie udostępnionej elektronicznej skrzynki podawczej (ESP). Dodał także, że MC nie wymaga podawania informacji o ESP od podmiotów posiadających ją w systemie ePUAP, ponieważ posiada już taką informację, a niewyłączenie usługi pomimo małego zainteresowania wynika z faktu, że ustawowy obowiązek informacyjny nadal istnieje.*

Ministerstwo Cyfryzacji podejmowało działania mające na celu uporządkowanie i aktualizację katalogu usług dostępnych na platformie ePUAP:

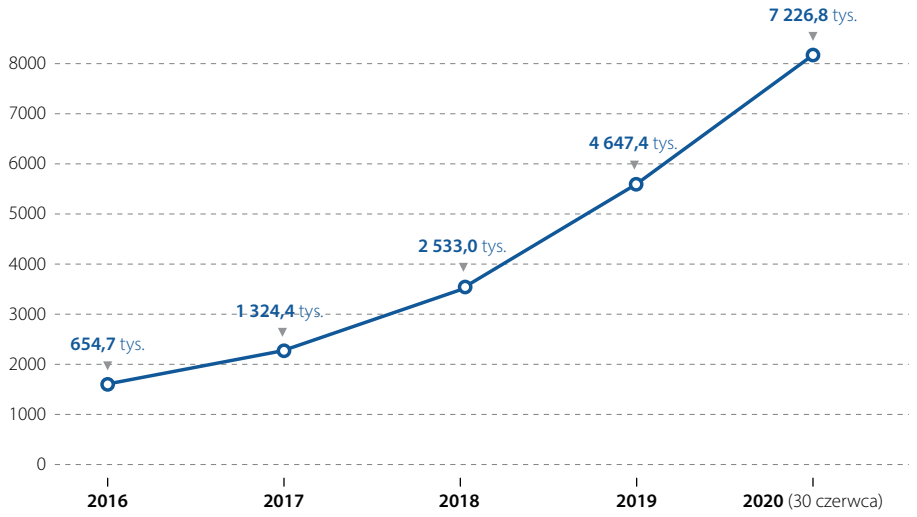
- w 2017 r. wysłano do 17 ministerstw pisma z prośbą o dokonanie aktualizacji e-usług dostępnych na platformie ePUAP lub wyłączenie usług nieaktywnych (otrzymano odpowiedź z 11 jednostek);
- w latach 2019–2020 (do czerwca), w związku z migracją usług na domenę gov.pl wspólnie z podmiotami udostępniającymi usługi ujednolicono sposób komunikowania o e-usługach w formie tzw. kart usług publicznych świadczonych elektronicznie[16];
- w grudniu 2019 r. wprowadzono procedurę stałej aktualizacji kart e-usług, w której uczestniczą podmioty je udostępniające (środowisko systemu zarządzania treścią GovPress jako narzędzie pracy dla redaktorów kart usług).

Działania informacyjne Ministra Cyfryzacji w celu zwiększenia liczby obywateli posiadających PZ

W okresie objętym kontrolą nastąpił ponad trzynastokrotny wzrost liczby obywateli posiadających profil zaufany. Liczba PZ zwiększyła się z 524,3 tys. (wg stanu na 1 stycznia 2016 r.) do 7226,8 tys. na dzień 30 czerwca 2020 r., tj. wzrosła o 1278,3%. Na koniec 2016 r. obywatele posiadali 654,7 tys. profili zaufanych, w 2017 r. – 1324,4 tys. (ponad dwukrotny wzrost w stosunku do roku 2016), w 2018 r. – 2533,0 tys. (wzrost o 1208,6 tys., tj. 91,2%), w 2019 r. – 4647,4 tys. (wzrost o kolejne 2114,4 tys., tj. o 83,5%). W pierwszej połowie roku 2020 liczba użytkowników PZ wzrosła o następne 2579,4 tys., tj. wzrost o 55,5% w stosunku do końca roku 2019.

[16] Karta usług to dedykowany punkt pierwszego kontaktu obywatela z e-usługą na portalu www.gov.pl.

Infografika nr 4
Liczba profili zaufanych w latach 2016–2020 (w tys.)



Źródło: opracowanie własne NIK na podstawie danych z kontroli.

W latach 2016–2017 działania promocyjno-informacyjne Ministra Cyfryzacji mające na celu zwiększenie zainteresowania profilem zaufanym skoncentrowały się na wykorzystaniu internetowych kanałów dotarcia do obywateli. Komunikaty w tym zakresie publikowane były na stronie internetowej Ministerstwa Cyfryzacji, a także na oficjalnych kanałach MC na YouTube, Facebook i Twitter. Informacje dotyczące profilu zaufanego przekazywano również podczas konferencji prasowych organizowanych z udziałem przedstawicieli Ministerstwa.

Dyrektor Generalny MC wyjaśnił, że upowszechnianie profilu zaufanego było także jednym z elementów działań odnoszących się do aplikacji mObywatel, mDokumenty oraz e-usług udostępnianych na portalu obywatel.gov.pl, a później na portalu gov.pl, gdyż posiadanie profilu zaufanego było warunkiem koniecznym skorzystania z tych usług.

W latach 2018–2020 głównym projektem promocyjno-informacyjnym MC dotyczącym profilu zaufanego były „Kampanie edukacyjno-informacyjne" (dalej: KEI), realizowane na podstawie porozumienia zawartego z Centrum Projektów Polska Cyfrowa. Projekt realizowany był wspólnie z Naukową Akademicką Siecią Komputerową – Państwowym Instytutem Badawczym (dalej: NASK-PIB) i Centrum Nauki Kopernik.

W ramach KEI prowadzono kampanie informacyjne dotyczące profilu zaufanego i e-usług, które publikowane były w mediach klasycznych, tj. telewizja, radio, prasa, a także w popularnych portalach internetowych[17] i mediach społecznościowych[18].

W sierpniu 2018 r. MC rozpoczęło współpracę z agencją Public Relations, której zadaniem było opracowanie strategii działań PR w zakresie KEI oraz realizacja ogólnopolskich kampanii mających na celu zwiększenie świadomości mieszkańców Polski w zakresie wykorzystania technologii telein-

[17] Interia.pl, wp.pl, onet.pl.

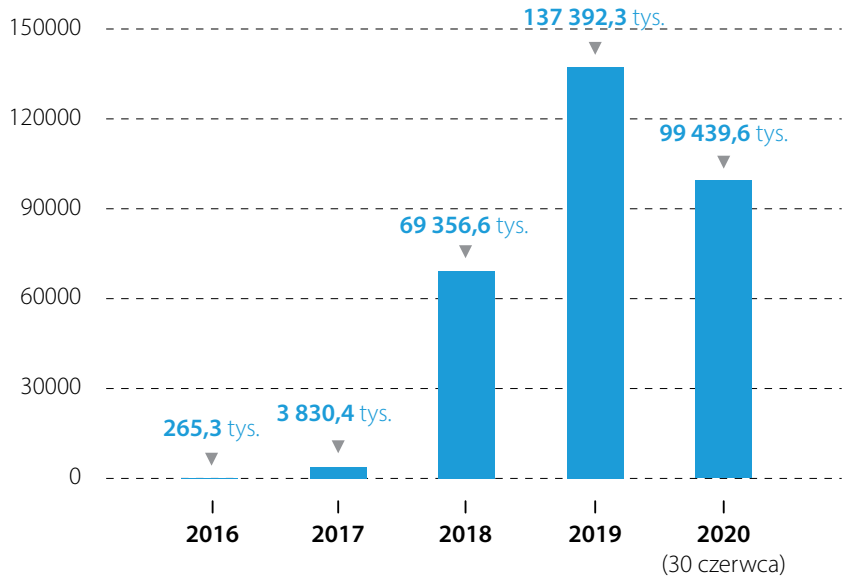
[18] Google, Facebook, Instagram, Youtube, LinkedIn, Twitter, inne uzgodnione kanały.

formatycznych w obszarze e-usług publicznych. W tym celu korzystano m.in. z tzw. Influencer marketingu, który polegał na prezentacji profilu zaufanego na blogach osób popularnych.

W ramach KEI, w sierpniu 2019 r., uruchomiono kampanię mediową, w której zachęcano do założenia profilu zaufanego i promującą e-usługi publiczne poprzez kampanie: #mamnowyprofil oraz e-Polak potrafi. Obejmowała ona media internetowe, prasę lokalną i ogólnopolską oraz radio i telewizję. Opublikowano także artykuły prasowe. Współtworzono również audycje telewizyjne i radiowe, w których zawarto wątki poświęcone profilowi zaufanemu i e-usługom, np. *Wielki test o Internecie w TVP, Dzień Dobry TVN*. Wątki poświęcone profilowi zaufanemu były także prezentowane w audycjach radiowych w Polskim Radiu i RMF FM. Działania realizowane były w ramach umów zawieranych przez MC, jak i przez partnera KEI – NASK-PIB.

W okresie objętym kontrolą następował systematyczny wzrost wykorzystywania profilu zaufanego przez obywateli w kontaktach z administracją. W roku 2016 profil zaufany został wykorzystany 1908,0 tys. razy. W 2017 r. PZ użyty został 10 087,6 tys. razy, tj. ponad czterokrotnie częściej niż w roku poprzednim (więcej o 428,7%). W latach 2018 i 2019 liczba operacji realizowanych z wykorzystaniem PZ wyniosła 18 820,4 tys. i 25 603,5 tys. (wzrost odpowiednio o 86,6% i 36,0% w ujęciu rok do roku). W pierwszej połowie 2020 r., z profilu zaufanego obywatele korzystali 20 870,0 tys. razy.

Infografika nr 5
Liczba e-usług zrealizowanych poprzez ePUAP w latach 2016–2020 (w tys.)



Źródło: opracowanie własne NIK na podstawie danych z kontroli.

W kwietniu 2020 r., w związku z epidemią COVID-19, MC uruchomiło możliwość założenia przez obywateli tymczasowego profilu zaufanego, którego ważność wynosiła trzy miesiące. Jego założenie możliwe było za pośrednictwem Internetu, bez konieczności wizyty w urzędzie, jak też bez konieczności uwierzytelnienia się za pośrednictwem systemów bankowych. Weryfikacja tożsamości następowała w formie video-rozmowy z urzędnikiem. **Do 30 czerwca 2020 r. założono 12,0 tys. tymczasowych profili zaufanych.**

W maju 2020 r. uruchomiona została aplikacja umożliwiająca założenie i potwierdzenie profilu zaufanego oraz logowanie do usług e-administracji z wykorzystaniem e-dowodu oraz technologii komunikacji bliskiego zasięgu w smartfonie – eDO App. Do dnia 2 lipca 2020 r. aplikację pobrano 44,0 tys. razy i dokonano 3,8 tys. potwierdzeń profilu zaufanego za pomocą e-dowodu, a do 9 lipca 2020 r. liczba logowań e-dowodem do usług administracji wyniosła 41,0 tys.

Wydatki związane z utrzymaniem ePUAP i PZ

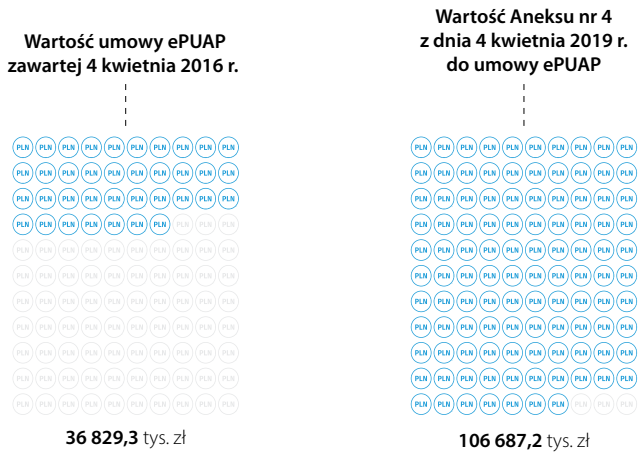
Świadczenie usług zapewniających poprawne i nieprzerwane funkcjonowanie ePUAP realizowane było na podstawie umowy zawartej 4 kwietnia 2016 r. pomiędzy Ministerstwem Cyfryzacji a COI[19] (dalej: umowa ePUAP). W latach 2016 i 2017 umowa ta obejmowała także utrzymanie systemu Profil Zaufany.

Umowa ePUAP została zawarta na okres 36 miesięcy (od 4 kwietnia 2016 r. do 4 kwietnia 2019 r.), a maksymalne wynagrodzenie obejmujące utrzymanie i prace dodatkowe ustalono w wysokości 36 829,3 tys. zł netto. W okresie objętym kontrolą, do umowy zawarto cztery aneksy[20].

Aneksem nr 4 z dnia 4 kwietnia 2019 r. do ww. umowy łączne maksymalne wynagrodzenie dla wykonawcy zwiększono do 106 687,2 tys. zł netto, tj. o 69 857,9 tys. zł (tj. o 189,7%) w porównaniu do pierwotnej umowy. Zwiększenie wynagrodzenia wynikało w szczególności:

- z wydłużenia okresu obowiązywania umowy o kolejne 36 miesięcy – do dnia 4 kwietnia 2022 r.,
- zwiększenia zakresu przedmiotu umowy poprzez dodanie kolejnego systemu – eUsługi obejmującego 18 usług zleconych do udostępnienia w interfejsie (gov.pl),
- zwiększenia kosztów usług utrzymania i usług dodatkowych wykazanego przez COI w kalkulacji wyceny umowy.

Infografika nr 6
Wzrost wartości umowy ePUAP



Źródło: opracowanie własne NIK na podstawie danych z kontroli.

[19] Umowa 1/P/DE/2016 (2/U/COI/MC/2016) na świadczenie usług zapewniających poprawne i nieprzerwane funkcjonowanie systemów: Elektronicznej Platformy Usług Administracji Publicznej, Scentralizowanego Systemu Dostępu do Informacji Publicznej, Strony Głównej Biuletynu Informacji Publicznej, Publikatora Aktów Prawnych .

[20] Aneks nr 1 z dnia 19 grudnia 2016 r., aneks nr 2 z dnia 29 grudnia 2017 r., aneks nr 3 z dnia 18 lutego 2019 r. oraz aneks nr 4 z dnia 4 kwietnia 2019 r.

Dyrektor Generalny MC wyjaśnił, że wprowadzenie dodatkowego systemu – eUsługi i udostępnienie usług w nowym interfejsie (gov.pl) miało na celu m.in. zwiększenie powszechności e-usług oraz poprawę jakości obsługi obywatela. Wskazał także, że zwiększenie wynagrodzenia z tytułu utrzymania systemu wynikało, obok wprowadzenia nowego systemu, także ze wzrostu liczby użytkowników ePUAP oraz ich aktywności w latach 2016–2019, a także ze wzrostu liczby zgłoszeń obsługiwanych przez Service Desk i skrócenia czasu obsługi incydentów krytycznych z trzech do jednego dnia roboczego.

Ministerstwo Cyfryzacji nie zapewniło niezależnej oceny sporządzonych przez COI kalkulacji zwiększających koszty umowy ePUAP skutkujących zwiększeniem wynagrodzenia wykonawcy, a także nie udokumentowało procesu negocjacji kosztów wynagrodzenia dla COI. Łączna wartość prac objętych aneksem nr 4 z dnia 4 kwietnia 2019 r. (po drugiej wycenie przez COI) wyniosła 106 687,2 tys. zł netto i była niższa o 5492,8 tys. zł netto, tj. o 4,9% od wyceny pierwotnej, która miała zwiększyć wynagrodzenie COI do 112 180,0 tys. zł netto. Do kontroli nie przedłożono żadnych dokumentów potwierdzających przeprowadzenie weryfikacji wyceny przez pracowników Ministerstwa lub przez niezależnych od COI ekspertów zewnętrznych.

Dyrektor Generalny wyjaśnił, że MC na bieżąco monitorowało i kontrolowało funkcjonowanie systemu ePUAP poprzez cotygodniowe spotkania dotyczące utrzymania systemów i posiadało wiedzę na temat pracochłonności. Dodatkowo wskazał, że każdorazowo w przypadku zawierania umów lub aneksów do nich MC organizuje spotkanie, na którym szczegółowo omawiana jest kalkulacja kosztów. Dodał także, że zapoznanie się z budową i zasadami funkcjonowania systemu ePUAP przez podmiot zewnętrzny wiązałoby się z bardzo dużym nakładem czasu oraz dodatkowymi kosztami dla MC. Dyrektor Generalny poinformował, że sporządzane w trybie roboczym notatki zawierające podsumowanie wątków poruszanych podczas spotkania są przechowywane w systemie sharepoint MC. Ze względu na ustawienia systemu, nie ma możliwości udostępnienia notatek z okresu od 1 stycznia do 30 kwietnia 2019 r. Natomiast notatka lub protokół ze spotkania z 2 kwietnia 2019 r. nie zostały sporządzone, gdyż wynikiem ustaleń była przygotowana przez COI ostateczna niższa wycena kosztów. Dyrektor Generalny wskazał również, że wycena przedstawiona przez COI była analizowana przez specjalistów MC i omówiona na spotkaniach operacyjnych. *Następnie ustnie przekazana dyrektorom Departamentu Systemów Państwowych oraz Departamentu Rozwoju Usług Cyfrowych*.

Zdaniem NIK w sytuacji gdzie Wykonawca samodzielnie sporządza kalkulację przedsięwzięcia, które będzie realizował, powinna być przeprowadzona niezależna od niego weryfikacja przyjętych kosztów, a wszystkie negocjacje, w których uczestniczą strony umowy, powinny zostać rzetelnie udokumentowane. W ocenie NIK, Minister Cyfryzacji powinien przeprowadzić rzetelną analizę kosztów przedstawionych w przedłożonej przez COI kalkulacji. Brak wyceny sporządzonej przez niezależnych od COI własnych lub zewnętrznych ekspertów i bazowanie wyłącznie na kalkulacji sporządzonej przez wykonawcę usługi było działaniem nierzetelnym.

Od 2018 r. utrzymanie Profilu Zaufanego realizowane było w ramach odrębnej umowy zawartej pomiędzy Ministrem Cyfryzacji a COI[21] (dalej: umowa PZ). Umowa PZ została zawarta na okres 36 miesięcy, tj. do 31 grudnia 2020 r. Maksymalne wynagrodzenie zostało określone w kwocie 14 854,5 tys. zł netto, w tym 8158,1 tys. zł netto ryczałtowej opłaty za realizację usług utrzymania.

W okresie od 1 stycznia 2016 r. do 30 czerwca 2020 r. w ramach umowy ePUAP, z tytułu utrzymania systemu zrealizowano wydatki w kwocie 62 747,4 tys. zł. Wydatki na utrzymanie Profilu Zaufanego w ramach umowy PZ zrealizowano w kwocie 12 041,9 tys. zł.

Nierzetelne ustalenie w umowach MC z COI mechanizmu/zasad pomiaru jakości obsługi zgłoszeń problemów przez użytkowników

W ww. umowach na utrzymanie systemów ePUAP oraz PZ został ustalony mechanizm pomiaru jakości obsługi zgłoszeń o problemach występujących w działaniu tych systemów, który nie uwzględniał wielkości przekroczenia wymaganego czasu obsługi, a jedynie sam fakt przekroczenia. Na potrzeby wyliczenia liczby zgłoszeń obsłużonych w danym miesiącu w terminie, COI przyjmowało jedynie zgłoszenia zakończone w danym miesiącu, przy czym nie uwzględniano wielkości przekroczenia wymaganego czasu obsługi, zatem mechanizm ten nie oddaje prawdziwego obrazu sytuacji w tym zakresie. W konsekwencji przykładowo w marcu 2020 r. **COI raportował do MC skuteczność obsługi zgłoszeń na poziomie 93,6% dla ePUAP, natomiast 96,2% dla PZ, mimo że w przypadku 76% incydentów dotyczących PZ i 63% incydentów dotyczących ePUAP ich obsługa nawet nie została rozpoczęta.**

Zbyt długie maksymalne czasy obsługi incydentów w umowach ePUAP i PZ

W umowie ePUAP i umowie PZ ustalono ponadto zbyt długie maksymalne czasy obsługi poszczególnych kategorii incydentów, co w konsekwencji wydłużało proces usuwania problemów. I tak, dla systemu ePUAP maksymalny czas na obsługę incydentu krytycznego w okresie od 30 marca 2016 r. do 4 kwietnia 2019 r. wynosił trzy dni robocze (od tej daty – jeden dzień roboczy). Natomiast czas obsługi incydentów pilnych zarówno dla systemu ePUAP, jak i PZ wynosił 10 dni roboczych, a incydentów standardowych – 20 dni roboczych. Zgodnie z ww. umowami dostępność danej usługi ePUAP i PZ była ustalana jako udział czasu obsługi incydentów krytycznych w danym miesiącu do całości wymaganego czasu jej dostępności, przy czym incydent krytyczny zdefiniowano jako awarię powodującą całkowity brak możliwości korzystania z głównych funkcji systemu ePUAP lub wszystkich usług wsparcia procesów biznesowych we wszystkich lokalizacjach w zakresie systemu PZ. Założenie, że poziom wskaźnika SLA ePUAP i PZ obniżają jedynie incydenty krytyczne, przy jednoczesnym wąskim zdefiniowaniu tego pojęcia, skutkowało tym, że raporty z utrzymania tych systemów w okresie poddanym kontroli nie odzwierciedlały ich rzeczywistej dostępności. W okresie objętym badaniem zdarzały się incydenty o statusie niższym niż krytyczne, które powodowały brak możliwości korzystania z tych systemów przez poszczególnych użytkowników zgodnie z ich przeznaczeniem, jednak nie były one uwzględniane przy obliczaniu raportowanego przez COI poziomu dostępności.

[21] Umowa nr 2/USiA/DUS/2017 z dnia 29 grudnia 2017 r. na świadczenie usług utrzymania i usług rozwoju systemów Profil Zaufany i Dostawca Tożsamości.

Rozwój ePUAP i PZ

W okresie objętym kontrolą, prace związane z rozwojem systemu ePUAP, realizowane był w ramach umowy ePUAP w formie *Świadczenia Usług Dodatkowych*. Do końca 2017 r. w związku z realizacją tej umowy, prowadzono także działania rozwojowe Profilu Zaufanego, który stanowił element systemu ePUAP. Od 2018 r., po wydzieleniu Profilu Zaufanego z ePUAP jako odrębnego systemu do autoryzacji i uwierzytelniania, prace rozwojowe PZ były realizowane na podstawie umowy PZ.

Uruchomienie prac rozwojowych ePUAP i PZ następowało na podstawie zleceń zgłaszanych COI przez MC. Rozliczenia wykonanej usługi dokonywano na podstawie podpisanego przez obie strony protokołu odbioru. Zarówno umowa ePUAP, jak i umowa PZ określały zasady zgłaszania, realizacji oraz rozliczania prac rozwojowych.

W ramach umowy ePUAP na rozwój systemu w okresie objętym kontrolą wydatkowano łącznie 5221,1 tys. zł (do 30 czerwca 2020 r.). W latach 2016 i 2017 wydatki te obejmowały także prace rozwojowe Profilu Zaufanego. Wydatki związane z rozwojem Profilu Zaufanego (w ramach umowy PZ) zrealizowane w latach 2018–2020 (do 30 czerwca) wyniosły 2510,9 tys. zł.

W okresie objętym kontrolą prace rozwojowe (modyfikacje) systemów ePUAP i PZ realizowane były także w ramach umowy ramowej na realizację projektu *Budowa Węzła Krajowego*[22] (dalej: umowa WK).

W ramach umowy WK zrealizowano sześć zleceń obejmujących swym zakresem modyfikacje ePUAP i PZ. W ofercie[23] do jednego z nich wyszczególniono kwotę 611,6 tys. zł, jako wydatki na modyfikację ePUAP, oraz kwotę 305,8 tys. zł jako wydatki na modyfikację PZ. W ofertach do pozostałych zleceń kwota dotycząca PZ nie została wyodrębniona i obejmowała także WK.

Dyrektor Generalny MC wyjaśnił, że modyfikacje systemów ePUAP i PZ zlecone w ramach umowy WK były ściśle powiązane z ich integracją z oprogramowaniem Węzła Krajowego, a ich testy wykonywano na środowisku testowym WK, co nie byłoby możliwe gdyby zlecenia były realizowane w ramach umowy ePUAP i umowy PZ. Poinformował także, że w latach 2019–2020 prace nad systemem ePUAP nie miały charakteru rozwojowego a jedynie miały na celu utrzymanie właściwego poziomu bezpieczeństwa systemu. Wskazał, że **trwają prace nad przeorganizowaniem ePUAP i przejęciem jego funkcjonalności przez inne systemy, takie jak gov.pl, Katalogi Administracji Publicznej, czy eDoręczenia**.

Według stanu na dzień 30 czerwca 2020 r. łączne wydatki na utrzymanie i rozwój w ramach umowy ePUAP zrealizowano w kwocie 67 968,5 tys. zł brutto. Wydatki obejmowały także utrzymanie i rozwój w latach 2016–2017 Profilu Zaufanego, który był elementem systemu ePUAP.

[22] Umowa ramowa nr 2/DUiRS/2017 z dnia 31 stycznia 2017 r. na realizację projektu pn. „Budowa Węzła Krajowego", dalej: Umowa WK.

[23] W § 3 umowy 2/DUiRS/2017 określono zasady zlecania prac COI. W ust. 2 i 3 zawarto postanowienia, że udzielenie zlecenia zostaje poprzedzone wnioskiem MC, w odpowiedzi na który COI przedstawia ofertę na realizację prac wraz z kalkulacją wynagrodzenia.

Łączne wydatki związane z Profilem Zaufanym, zrealizowane w latach 2018–2020 w ramach umowy PZ wyniosły 14 552,8 tys. zł brutto.

Działania MC na rzecz realizacji celu w zakresie e-usług określonego w SOR

Minister Cyfryzacji realizował cel jakim było *stworzenie cyfrowego państwa usługowego poprzez udostępnienie wysokiej jakości usługi na rzecz obywateli, w tym również przedsiębiorców, które mają być zapewniane przez nowoczesne rozwiązania informatyczne wspierające logiczny i spójny system informacyjny państwa, zbudowany i utrzymywany przy współpracy wszystkich podmiotów na różnych szczeblach administracji publicznej.* Cel ten określono w *Strategii na rzecz Odpowiedzialnego Rozwoju do roku 2020 (z perspektywą do 2030 r.)*[24] dla obszaru *E-państwo*. W SOR w obszarze *E-państwo*[25] ujęto dla Ministra Cyfryzacji priorytetowe zadanie *Udostępnienie jak najszerszego zakresu usług publicznych świadczonych elektronicznie, umożliwiających obywatelowi załatwienie danej sprawy na odległość*. W związku z realizacją tego zadania w SOR zaplanowano podjęcie 13 działań (dziesięć z nich zostało objęte niniejszą kontrolą[26]).

Dyrektor Generalny MC wyjaśnił, że *działania zapisane w SOR, za których realizację odpowiada Minister Cyfryzacji mieszczą się w zakresie działalności ministra właściwego ds. informatyzacji. W związku z powyższym, działania te znajdują się w zakresie zadań przypisanych komórkom organizacyjnym Ministerstwa, w Regulaminie organizacyjnym MC oraz w poszerzonej formie w ich wewnętrznych regulaminach organizacyjnych*. W odniesieniu do niesporządzenia harmonogramu, Dyrektor Generalny MC podał, że *z zapisów Strategii nie wynika obowiązek tworzenia harmonogramu dla innych działań zapisanych w SOR, a zatem należy przyjąć, że powinny one zostać zrealizowane do roku 2030. (...) opis kluczowych, zdaniem MC, zadań Ministra Cyfryzacji, które wiążą się z realizacją działań opisanych w SOR wraz z ramami czasowymi ich realizacji jest przygotowywany każdego roku w ramach Planu działalności Ministra Cyfryzacji. Szczegółowe harmonogramy określane są dla każdego projektu z osobna.* Odnosząc się do nieokreślenia szczegóło-

---

[24] Dokument przyjęty uchwałą Rady Ministrów z dnia 14 lutego 2017 r.

[25] Kierunek interwencji *Budowa i rozwój e-administracji – orientacja administracji państwa na usługi cyfrowe.*

[26] Działania objęte kontrolą:
- zapewnienie e-usług adekwatnych do realnych potrzeb, zgłaszanych przez obywateli i przedsiębiorców;
- stworzenie jednego portalu informacji i e-usług administracji rządowej w celu sprawniejszego dostępu dla obywateli i przedsiębiorców;
- wprowadzenie jednolitego i bezpiecznego schematu identyfikacji obywateli (eID) w systemach e-usług administracji publicznej;
- zapewnienie dominującego udziału elektronicznego obiegu dokumentów w administracji i obrocie gospodarczym (Paperless);
- przyjęcie standardu systemów elektronicznego zarządzania dokumentacją (EZD) w administracji, gwarantującego sprawną wymianę informacji/danych z systemami dziedzinowymi administracji publicznej;
- zintegrowanie infrastruktury przetwarzania danych e-administracji i rozwój Systemu Rejestrów Państwowych (SRP);
- zapewnienie niezbędnej niezawodności i dostępności systemów e-administracji oraz ich integracja;
- stworzenie efektywnego systemu zarządzania zasobami informacyjnymi administracji;
- budowa kompetencji cyfrowych administracji, zarówno technicznych, jak i dotyczących praktycznego stosowania technologii cyfrowych;
- zastosowanie instrumentów analitycznych służących identyfikacji potrzeb obywateli w ramach e-administracji oraz wspieraniu działań podnoszących aktualność i wiarygodność danych znajdujących się w rejestrach państwowych.

wych zasad monitoringu i jego częstotliwości w zakresie działań przypisanych Ministerstwu w SOR, Dyrektor Generalny MC podał, że *zapisy Strategii nie nakładają na resorty obowiązku tworzenia dodatkowych form i zasad monitorowania realizacji działań.*

Projektami strategicznymi realizowanymi przez Ministra w ramach SOR były:

- ***Program Zintegrowanej Informatyzacji Państwa*** – stworzenie spójnego, logicznego i sprawnego systemu informacyjnego państwa, zapewniającego przejrzystość funkcjonowania administracji i dostarczającego na poziomie wewnątrzkrajowym i europejskim usługi kluczowe dla obywateli i przedsiębiorców, w sposób efektywny kosztowo i jakościowo oraz zapewnienie interoperacyjności istniejących oraz nowych systemów teleinformatycznych administracji publicznej (w tym wyeliminowanie powielających się funkcjonalności);
- projekt pn. ***Poczta Polska jako strategiczny filar państwa w rozwoju e-governement*** – rozbudowa e-usług przez operatora pocztowego Poczta Polska S.A. (na platformie Envelo) w ramach projektu przyspieszenia cyfryzacji i stworzenia platformy elektronicznej relacji państwo–obywatel.

Dyrektor Generalny MC poinformował, że monitoring projektów strategicznych wskazanych w SOR, za których realizację odpowiada Minister Cyfryzacji, prowadzony był w trybie miesięcznym w systemie MonAliza[27]. Poinformował również, że działania MC znajdujące się w zakresie objętym kontrolą NIK monitorowane były również m.in. przez Komitet Rady Ministrów do spraw Cyfryzacji (kwartalnie). Ponadto realizacja działań wskazanych w SOR monitorowana była w ramach przeglądów realizacji SOR dokonywanych przez Ministerstwo Funduszy i Polityki Regionalnej.

Z kart monitoringu strategicznego za lata 2017–2019 (kwartalnych i rocznych) oraz *Sprawozdania z realizacji ‚Strategii na rzecz Odpowiedzialnego Rozwoju' w 2019 r.*[28] wynika, że Minister Cyfryzacji terminowo realizował projekty SOR (PZIP oraz Poczta Polska jako strategiczny filar państwa w rozwoju usług e-goverment). W maju 2020 r. Ministerstwo konsultowało, w ramach Komitetu Koordynacji Polityki Rozwoju, dokument dotyczący przeglądu śródokresowego I etapu realizacji SOR. W dokumencie tym odniesiono się m.in. do obszaru *E-państwo*, wskazując wyróżniające się projekty, w tym rozwój e-Państwa i cyfryzacja procesów (uruchamianie nowych e-usług np. e-dowód, e-Protokoły[29], e-Doręczenia[30], e-Zwolnienia) oraz wprowadzenie kolejnych modułów w ramach rządowej aplikacji mobilnej mObywatel, mTożsamość, mPojazd, mLegitymacja szkolna, mLegitymacja studencka, eRecepta, Polak za granicą oraz aplikację mWeryfikator[31].

[27] W systemie MonAliza raportuje się główne prace służące tworzeniu, modyfikacji i rozwojowi e-usług.

[28] Opracowane przez Ministerstwo Funduszy i Polityki Regionalnej (Warszawa, maj 2020 r.).

[29] Protokoły elektroniczne w sądach powszechnych.

[30] Usługi rejestrowanego doręczenia elektronicznego w Polsce.

[31] Bezpłatna i oficjalna rządowa aplikacja na smartfony umożliwiająca potwierdzenie danych osoby korzystającej z aplikacji mObywatel.

Koordynacją działań związanych z realizacją SOR w Ministerstwie Cyfryzacji zajmował się Departament Architektury Informacyjnej Państwa (DAIP), do zadań którego należało m.in. *kreowanie polityki w obszarze budowy i rozwoju e-Administracji, w tym w zakresie elektronicznego zarzadzania dokumentacją, prowadzenie spraw związanych z wdrażaniem i monitorowaniem realizacji Programu Zintegrowanej Informatyzacji Państwa.* Dyrektor Generalny MC podał, *że za realizację celu zadania Udostępnienie jak najszerszego zakresu usług publicznych świadczonych elektronicznie (...) odpowiada Ministerstwo Cyfryzacji, jako całość, tj. komórki wykonujące zadania merytoryczne wg swojej właściwości. Jednak odpowiedzialność za działania w ramach udostępniania usług publicznych świadczonych elektronicznie spoczywa na wszystkich członkach Rady Ministrów.*

Zgodnie z założeniami SOR, wszystkie działania wskazane w kierunku interwencji *Budowa i rozwój e-administracji – orientacja administracji państwa na usługi cyfrowe* powinny skutkować wzrostem wskaźnika *odsetek osób korzystających z Internetu w kontaktach z administracją publiczną do przekazywania wypełnionych formularzy*[32]. Na koniec 2019 r. wartość tego wskaźnika wyniosła 31,4%[33]. Dyrektor Generalny w wyjaśnieniach podał, że poziom realizacji wskaźnika w poprzednich latach kształtował się następująco: w 2016 r. – 18,8%; w 2017 r. – 21,0%; w 2018 r. – 24,6%, a w 2019 r. – 31,4%, więc przewiduje się osiągnięcie wskaźnika zakładanego na koniec 2020 r. (tj. 32,0%). Celem Ministra Cyfryzacji w ramach zadania wskazanego w SOR była także prezentacja ujednoliconych kart usług świadczonych publicznie. Według stanu na 30 czerwca 2020 r. Ministerstwo we współpracy z właścicielami usług udostępniało na Portalu RP (www.gov.pl) 387 kart usług publicznych świadczonych elektronicznie. Uruchomienie części transakcyjnej Portalu (www.gov.pl)[34] nastąpiło 30 września 2019 r.

Minister Cyfryzacji realizował także zadania służące osiągnięciu celu głównego Programu Zintegrowanej Informatyzacji Państwa[35], tj. *modernizacja administracji publicznej z wykorzystaniem technologii cyfrowych nakierowana na potrzebę podniesienia sprawności państwa i poprawienie jakości relacji administracji z obywatelami i innymi interesariuszami*. Zgodnie z PZIP, głównymi beneficjentami działań na rzecz transformacji cyfrowej mają być obywatele, którzy dzięki niej zyskają dostęp do wysokiej jakości zaawansowanych e-usług świadczonych przez administrację publiczną. Po zmianach,

---

[32] Wskaźnik ten, zgodnie z SOR, powinien wzrosnąć z poziomu 16% w 2015 r. (wartość bazowa) do 32% w 2020 r. i 40% w 2030 r.

[33] Źródło danych GUS: Społeczeństwo informacyjne w Polsce. Wyniki badań statystycznych z lat 2015–2019.

[34] Portal gov.pl obecnie przejął funkcję serwisu obywatel.gov.pl i ePUAP, i jest główną bramą do informacji i e-usług Polski. Średniomiesięcznie serwis jest odwiedzany przez 10–26 mln użytkowników.

[35] Program przyjęty Uchwałą nr 1/2014 Rady Ministrów z dnia 8 stycznia 2014 r. *w sprawie przyjęcia programu rozwoju „Program Zintegrowanej Informatyzacji Państwa"* (RM-111-241-13), zmieniony: Uchwałą nr 117/2016 2014 Rady Ministrów z dnia 27 września 2016 r. *zmieniającą uchwałę w sprawie przyjęcia programu rozwoju „Program Zintegrowanej Informatyzacji Państwa"* (RM-111-120-16) oraz Uchwałą nr 109/2019 Rady Ministrów z dnia 24 września 2019 r. *zmieniającą uchwałę w sprawie przyjęcia programu rozwoju „Program Zintegrowanej Informatyzacji Państwa"* (RM-111-111-19).

okres realizacji PZIP został wydłużony z końca 2020 r. na koniec 2022 r. W 2019 r. w załączniku nr 2 do PZIP został dodany plan działań, zawierający 122 projekty planowane do realizacji przez 17 resortów i inne instytucje (dla MC zaplanowane było 17 projektów, z tego osiem związanych z szerokorozumianymi e-usługami[36]). W okresie od 22 kwietnia do 15 maja 2020 r. przeprowadzono proces zbierania danych dotyczących aktualizacji statusu projektów obowiązujących w PZIP oraz zgłoszenia nowych przedsięwzięć. W wyniku tego liczba projektów zwiększyła się o kolejne 100.

Minister Cyfryzacji uczestniczył w realizacji trzech celów szczegółowych PZIP:
- celu szczegółowego nr 1 – *Zwiększenie jakości oraz zakresu komunikacji między obywatelami i innymi interesariuszami a państwem*;
- celu szczegółowego nr 2 – *Wzmocnienie dojrzałości organizacyjnej jednostek administracji publicznej oraz usprawnienie zaplecza elektronicznej administracji (back office)*;
- celu szczegółowego nr 3 – *Podniesienie poziomu kompetencji cyfrowych obywateli, specjalistów TIK oraz pracowników administracji publicznej*.

Dyrektor Generalny MC poinformował, że jednym z działań Ministra Cyfryzacji prowadzącym do realizacji celów szczegółowych 1 i 2 było *definiowanie Architektury Informacyjnej Państwa w szczególności przygotowanie Wizji i Modelu Architektury Informacyjnej Państwa. Wizja AIP jest definicją sposobu organizacji systemów służących realizacji e-usług, która wspiera gestorów systemów teleinformatycznych państwa w podnoszeniu dostępności i interoperacyjności tych systemów. Standardy i pryncypia, przygotowywane w ramach modelu AIP określają sposób wdrażania rozwiązań dla administracji. Wizja AIP zawiera również generyczny proces realizacji e-usług publicznych (...), które powinny być zmodyfikowane lub zbudowane. Dotyczy zarówno jednostek centralnych jak i samorządowych.* Dyrektor podał również, że *moduły/systemy zdefiniowane przez AIP powstają w projektach (Katalogi Administracji Publicznej, portal GOV,pl, Zintegrowanej Platformy Analitycznej, System Rejestrów Państwowych, e-Doręczenia, EZD RP – elektroniczne zarządzanie dokumentacją w administracji publicznej).*

Zgodnie z PZIP odpowiedzialność za rezultaty Programu spoczywała na wszystkich członkach Rady Ministrów, a Minister Cyfryzacji był odpowiedzialny za koordynację realizacji PZIP jako całości.

[36] Działania w PZIP związane z realizacją e-usług (wg załącznika nr 2):
1) Optymalizacja i rozwój Portalu gov.pl;
2) Budowo i rozwój e-usług;
3) Rozwój publicznej aplikacji mobilnej (mObywatel);
4) Wdrożenie platformy API – Cyfrowej Piaskownicy Administracji wraz z procedurami jej funkcjonowania jako narzędzia społecznościowego rozwoju usług cyfrowych wraz z testami na trzech zaplanowanych inicjatywach;
5) Wdrożenie projektu informatycznego e-Doręczenia – usługa rejestrowanego doręczenia elektronicznego w Polsce;
6) Udostępnienie jednolitego systemu EZD RP, który ma być nowoczesnym i uniwersalnym narzędziem do elektronicznego zarządzania dokumentacją, powszechnie użytkowanym w jednostkach administracji publicznej, wyznaczającym standard dla tej klasy systemów;
7) Rozwój Systemu Rejestrów Państwowych;
8) Wdrożenie projektu Katalogi Administracji Publicznej.

Efekty realizacji celów szczegółowych PZIP były monitorowane w oparciu o ustalone w PZIP wskaźniki, których osiągnięcie było zaplanowane na koniec 2022 r. Według stanu na koniec 2019 r. wartość wskaźnika:

1) *poziom zorientowania na użytkownika e-usług* wyniosła 84,8% wobec 85,0% planowanych na koniec 2022 r.;
2) *odsetek osób korzystających z Internetu w kontaktach z administracją publiczną* została osiągnięta na poziomie 40,4% wobec 50% planowanych na koniec 2022 r.;
3) *odsetek urzędów administracji państwowej korzystających z systemu elektronicznego zarządzania dokumentacją jako podstawowego sposobu dokumentowania przebiegu załatwiania i rozstrzygania spraw* wyniosła 63,7% wobec 75% planowanych na koniec 2022 r.;
4) *udział dokumentów elektronicznych wysyłanych przy wykorzystaniu elektronicznej skrzynki podawczej w korespondencji wychodzącej z urzędów administracji państwowej* wyniosła 9,1% przy planowanych 55% na koniec 2022 r.;
5) *odsetek osób posiadających profil zaufany* została osiągnięta w wysokości 14,8% wobec 35% planowanych na koniec 2022 r.;
6) *odsetek osób posiadających podstawowe lub ponadpodstawowe umiejętności cyfrowe* wyniosła 44,2% wobec 56% planowanych na koniec 2022 r.

Realizacja przez MC działania określonego w SOR pn. *Zapewnienie e-usług adekwatnych do realnych potrzeb, zgłaszanych przez obywateli i przedsiębiorców*

Celem określonego w SOR działania pn. *Zapewnienie e-usług adekwatnych do realnych potrzeb, zgłaszanych przez obywateli i przedsiębiorców* było upowszechnienie i wspieranie rozwoju e-usług publicznych/umożliwienie obywatelom, przedsiębiorcom oraz administracji publicznej załatwiania spraw urzędowych drogą elektroniczną. Według stanu na 30 czerwca 2020 r. Minister udostępnił łącznie 30 e-usług centralnych, w tym 22 w okresie kontrolowanym.

Realizacja przez MC działania określonego w SOR pn. *Stworzenie jednego portalu informacji i e-usług administracji rządowej w celu sprawniejszego dostępu dla obywateli i przedsiębiorców*

Celem działania pn. *Stworzenie jednego portalu informacji i e-usług administracji rządowej w celu sprawniejszego dostępu dla obywateli i przedsiębiorców* było *ustandaryzowanie i ułatwienie prowadzenia stron informatycznych kolejnym jednostkom administracji i podmiotom wykonującym zadania publiczne, w ramach modernizacji Portalu RP*[37]. Według stanu na 30 czerwca 2020 r. na stronie Portalu RP (www.gov.pl) opublikowano serwisy informacyjne 39 urzędów, w tym: 19 ministerstw, KPRM, czterech urzędów wojewódzkich, 10 urzędów centralnych.

Realizacja przez MC działania określonego w SOR pn. *Wprowadzenie jednolitego i bezpiecznego schematu identyfikacji obywateli (eID) w systemach e-usług administracji publicznej*

Celem działania pn. *Wprowadzenie jednolitego i bezpiecznego schematu identyfikacji obywateli (eID) w systemach e-usług administracji publicznej* było *wprowadzenie krajowego schematu identyfikacji elektronicznej jako wspólnej podstawy dla bezpiecznej interakcji elektronicznej między obywa-*

[37] Projekt Portal RP jest kontynuacją prac na rzecz budowy spójnego systemu informacyjnego (gov.pl) dla całej administracji – cyfrowej bramy, udostępniającej każdego typu informacje i e-usługi oferowane przez administrację publiczną. W ramach prowadzonych prac w projekcie – przewidzianych do 2021 r. – migrowane będą strony urzędów centralnych, wojewódzkich i samorządowych. Rozbudowywany zostanie system do zarządzania treścią, który pozwoli redaktorom z urzędów centralnych, wojewódzkich i samorządowych na coraz wygodniejsze zarządzanie i aktualizowanie treści poszczególnych podmiotów.

telami, przedsiębiorstwami i organami publicznymi w celu upowszechnienia usług online wymagających uwierzytelnienia.

Działanie to było wykonywane poprzez realizację projektu *Budowa i wdrożenie krajowego węzła identyfikacji elektronicznej* oraz projektu *Rozwój Cyfrowej Tożsamości*, w ramach których:

- uruchomiono Węzeł Krajowy (WK)[38] jako podstawę dla bezpiecznej komunikacji elektronicznej między obywatelami, przedsiębiorstwami i organami publicznymi w celu upowszechnienia usług online wymagających uwierzytelnienia;
- stworzono model identyfikacji elektronicznej i wdrożono interoperacyjne rozwiązanie jakim jest WK, dotyczący transakcji oraz danych obywateli i podmiotów wykorzystujących systemy identyfikacji elektronicznej;
- wprowadzono wspólny standard dla interfejsów, zgodny z wymaganiami rozporządzenia eIDAS[39], co zminimalizowało ryzyko związane z nieuprawnionym dostępem do danych identyfikacyjnych;
- spełniono wymagania prawne wynikające z rozporządzenia eIDAS, tj. stworzono warunki techniczno-organizacyjne poprzez budowę i uruchomienie produkcyjne Węzła Transgranicznego, który jest gotowy do przekazywania notyfikowanych środków identyfikacji elektronicznej do e-usług administracji publicznej w UE i w Polsce;
- wraz z wdrożeniem e-dowodu został wdrożony System Identyfikacji Elektronicznej (SIE), w ramach którego wydawany jest profil osobisty, czyli środek identyfikacji, którym może posługiwać się posiadacz e-dowodu. System został zintegrowany z Węzłem Krajowym i bierze udział w procesie identyfikacji jako system identyfikacji elektronicznej. W maju 2020 r. SIE został zintegrowany z aplikacją eDO App w celu umożliwienia obywatelom dostępu do e-usług administracji publicznej z wykorzystaniem e-dowodu i aplikacji mobilnej eDO App na telefony z NFC.

Realizacja przez MC działania określonego w SOR pn. *Zapewnienie dominującego udziału elektronicznego obiegu dokumentów w administracji i obrocie gospodarczym* (Paperless)

Jak wyjaśnił Dyrektor Generalny MC, w ramach działania pn. *Zapewnienie dominującego udziału elektronicznego obiegu dokumentów w administracji i obrocie gospodarczym (Paperless)*, MC przygotowuje *projekt ustawy paperless, która określi szczegółowe daty wdrażania kolejnych rozwiązań w obszarze elektronizacji. Wśród propozycji znajdują się kolejne procesy, które mogą być realizowane transakcyjnie. Ustawa prawo o aktach stanu cywilnego przewiduje od 1 stycznia 2023 r. wydawanie elektronicznej karty zgonu. W trzecim kwartale 2020 r. wdrożona zostanie także usługa zgłoszenia unieważnienia dowodu osobistego na skutek tzw. kradzieży tożsamości.* Ponadto poinformował, że monitorowanie wykorzystania wdrażanych

[38] Węzeł krajowy to rozwiązanie organizacyjno-techniczne umożliwiające uwierzytelnianie użytkownika systemu teleinformatycznego, korzystającego z usługi online, z wykorzystaniem środka identyfikacji elektronicznej wydanego w systemie identyfikacji elektronicznej przyłączonym do tego węzła bezpośrednio albo za pośrednictwem węzła transgranicznego.

[39] 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 uchylające dyrektywę 1999/93/WE (Dz. Urz. UE L 257 z 28.08.2014, s. 73, ze zm.).

rozwiązań odbywa się m.in. przez analizę liczby osób dopisanych do Rejestru Danych Kontaktowych[40], czy liczbę pobranych przy użyciu udostępnionej usługi odpisów aktu stanu cywilnego. Podał, że w ramach działania wdrożono nowe usługi o wyższym stopniu dojrzałości (GOV), tzw. usługi transakcyjne, np. unieważnienie dowodu osobistego na skutek zgłoszenia jego utraty. Usługi transakcyjne skracają czas realizacji e-usługi, obniżają jej koszty, a także umożliwiają użytkownikowi dokonanie zgłoszenia i odnotowanie zdarzenia w dowolnym czasie i godzinie. Poinformował, że rozwijane są usługi bazujące na możliwości samodzielnego pobrania dokumentów, np. odpisu aktu stanu cywilnego czy informacji o zameldowaniu, które opatrzone będą kwalifikowaną pieczęcią Ministra.

Realizacja przez MC działania określonego w SOR pn. *Przyjęcie standardu systemów elektronicznego zarządzania dokumentacją (EZD) w administracji, gwarantującego sprawną wymianę informacji/danych z systemami dziedzinowymi administracji publicznej*

Działanie pn. *Przyjęcie standardu systemów elektronicznego zarządzania dokumentacją (EZD) w administracji, gwarantującego sprawną wymianę informacji/danych z systemami dziedzinowymi administracji publicznej*, realizowane było w ramach projektu *EZD–RP elektroniczne zarządzanie dokumentacją w administracji publicznej*[41]. Liderem odpowiedzialnym za realizację projektu był NASK-PIB (beneficjent projektu w ramach Programu Operacyjnego Polska Cyfrowa, dalej: POPC), który realizuje go w partnerstwie z Podlaskim Urzędem Wojewódzkim. Dyrektor Generalny MC poinformował, że rolę tę przejmie Ministerstwo Cyfryzacji.

Z *Raportu z postępu rzeczowo-finansowego projektu informatycznego za II kwartał 2020 r.* wynika, że w ramach projektu zamknięto listy funkcjonalności systemu (31 marca 2019 r.) oraz przygotowano pierwszą wersję prototypu systemu (30 września 2019 r.). Dyrektor Generalny poinformował, że *projekt jest w trakcie realizacji, osiągniecie rezultatów jest planowane na koniec 2021 r.*

Realizacja przez MC działania określonego w SOR pn. *Zintegrowanie infrastruktury przetwarzania danych e-administracji i rozwój Systemu Rejestrów Państwowych (SRP)*

Działanie pn. *Zintegrowanie infrastruktury przetwarzania danych e-administracji i rozwój Systemu Rejestrów Państwowych (SRP)* realizowane było w ramach projektu *Rozwój Systemów Rejestrów Państwowych*[42]. Dyrektor Generalny MC wyjaśnił, że *praca dedykowana rozwojowi SRP zorganizowana została w kilku grupach roboczych poświęconych poszczególnym komponentom, w których pracach udział biorą przedstawiciele MC, MSWiA, wykonawcy, a także samorządu (z USC). Spotkania grup roboczych odbywają się co 2 tygodnie. Podczas prac grup omawiane są bieżące problemy w funkcjonowaniu SRP i proponowane ich rozwiązania. Praca w ramach projektu Rozwoju SRP finansowanego z PO PC monitorowana jest na bieżąco poprzez cotygodniowe statusy z udziałem beneficjenta i partnera projektu.*

---

[40] Rejestr danych kontaktowych osób fizycznych prowadzi w systemie teleinformatycznym minister właściwy do spraw informatyzacji. Przekazanie danych osobowych do RDK przez osobę, której dane dotyczą jest całkowicie dobrowolne, a przetwarzanie danych w tym rejestrze odbywa się na podstawie zgody udzielonej przez tę osobę. Przekazane do RDK dane osoba, której dane dotyczą, może je w każdej chwili usunąć, bądź dokonać zmiany przekazanych danych w zakresie numeru telefonu komórkowego i adresu poczty elektronicznej.

[41] Data rozpoczęcia projektu 1 stycznia 2019 r., planowana data zakończenia 31 grudnia 2021 r.

[42] Data rozpoczęcia projektu 29 marca 2018 r., planowana data zakończenia 28 marca 2021 r.

W ramach Rozwoju SRP podjęte zostały m. in. następujące działania:

- przygotowano system SRP do wydawania e-dowodów oraz wdrożono e-usługi związane z e-dowodem:
- usługa wnioskowania o dowód osobisty – posiadacza lub innej osoby,
- usługa transakcyjna zawieszania/cofania certyfikatów posiadacza dowodu osobistego,
- usługa nietransakcyjna zawieszania/cofania zawieszenia certyfikatów dowodu osobistego – dla dziecka, podopiecznego lub innej osoby,
- usługa „Sprawdź, czy dowód jest unieważniony lub zawieszony",
- usługa „Sprawdź swoje dane w Rejestrze Dowodów Osobistych",
- usługa „Zgłoś utratę albo uszkodzenie dowodu osobistego (unieważnienie dowodu osobistego)" dziecka lub podopiecznego (marzec 2019 r.);
- uruchomiono usługę zakładania i potwierdzania online Profilu Zaufanego e-dowodem (czerwiec 2019 r.);
- kontynuowano działania związane z parentyzacją[43] (na koniec 2019 r. osiągnięto poziom bliski 100%);
- w ramach rejestru PESEL wdrożono usługę polegającą na zgłaszaniu niezgodności do właściwych organów;
- przygotowano modyfikację Rejestru Dowodów Osobistych (RDO) związaną z tzw. „kradzieżą tożsamości" (wdrożenie zmian nastąpiło 12 stycznia 2020 r.);
- wdrożono funkcjonalności umożliwiające wydawanie formularzy wielojęzycznych z poziomu Źródła – aplikacji do obsługi SRP;
- wdrożono zmiany ustawy o ewidencji ludności w przedmiocie udostępniania danych tj. „licznik 300" dla udostępnień podmiotom publicznym[44], a także zaimplementowano słownik podmiotów publicznych;
- zapewniono organom wojewódzkim wgląd do Rejestru Dowodów Osobistych;
- prowadzono prace analityczne i developerskie związane z uruchomieniem nowego Rejestru Dokumentów Paszportowych, który będzie elementem SRP;
- 22 grudnia 2019 r. uruchomiono Rejestr Danych Kontaktowych umożliwiający korzystanie z e-usług online (przekazanie, zmiana i usuniecie danych oraz potwierdzenie swoich danych do RDK) wraz z e-usługami dedykowanymi RDK bezpośrednio przez obywateli poprzez aplikację Źródło i WebService. W RDK zarejestrowano już ponad 2,5 mln osób;
- uruchomiono usługi pobrania: odpisu aktu stanu cywilnego oraz informacji o adresie zameldowania.

[43] Parentyzacja to funkcja w Systemie Rejestrów Państwowych, która umożliwia automatyczne tworzenie powiązań dziecka z rodzicami poprzez PESEL.

[44] Od 1 maja 2019 r. zgodnie z art. 48 ust. 2 ustawy o ewidencji ludności (Dz. U. z 2019 r. poz. 1397, ze zm.) podmioty publiczne, które nie posiadają decyzji administracyjnej, na podstawie której uzyskały dostęp do rejestru PESEL/rejestru mieszkańców za pomocą urządzeń teletransmisji danych, w danym roku kalendarzowym mogą uzyskać maksymalnie 300 danych jednostkowych z rejestru PESEL albo 300 danych jednostkowych odrębnie z każdego lokalnego rejestru mieszkańców, który jest prowadzony zgodnie z właściwością miejscową przez dany organ gminy (tzw. licznik 300).

Realizacja przez MC działania określonego w SOR pn. *Zapewnienie niezbędnej niezawodności i dostępności systemów e-administracji oraz ich integracja*

W ramach działania pn. *Zapewnienie niezbędnej niezawodności i dostępności systemów e-administracji oraz ich integracja* realizowano dwa cele:

– *zapewnienie spójnej, uporządkowanej, dostępnej również dla osób niepełnosprawnych bramki do zasobów państwa polskiego* (realizowany przez Departament Rozwoju Usług (projekt Portal RP)). W ramach tego celu na portalu gov.pl opublikowano serwisy informacyjne 39 urzędów (spośród 118 planowanych – termin realizacji do kwietnia 2022 r.). Zapewniono wszystkim użytkownikom możliwość korzystania z portalu gov.pl, w tym osobom niepełnosprawnym (niewidomym, słabowidzącym, z ograniczoną motoryką),
– *wsparcie w rozwiązywaniu istniejących problemów w interoperacyjności rejestrów publicznych i głównych systemów informatycznych państwa, poprzez opracowanie i wdrożenie zarządzania architekturą danych państwa (m.in. przez opracowanie rekomendacji architektonicznych w zakresie gromadzenia, udostępniania i wymiany danych),* realizowany przez Zespół AIP[45] Departamentu Architektury Informacyjnej Państwa łącznie z opisanym poniżej działaniem *Stworzenie efektywnego systemu zarządzania zasobami informacyjnymi administracji*.

Realizacja przez MC działania określonego w SOR pn. *Stworzenie efektywnego systemu zarządzania zasobami informacyjnymi administracji*

Celem działania pn. *Stworzenie efektywnego systemu zarządzania zasobami informacyjnymi administracji*, było *wsparcie w rozwiązywaniu istniejących problemów w interoperacyjności rejestrów publicznych i głównych systemów informatycznych państwa, poprzez opracowanie i wdrożenie zarządzania architekturą danych państwa (m.in. przez opracowanie rekomendacji architektonicznych w zakresie gromadzenia, udostępniania i wymiany danych).* Dyrektor Generalny MC podał, że monitorowanie tych dwóch celów odbywało się poprzez: spotkania statusowe i raportowanie; prezentacje wyników prac na Radzie Architektury IT Komitetu Rady Ministrów ds. Cyfryzacji[46]; prezentacje w ramach prac grupy roboczej architektury danych MC; konsultacje i weryfikacja wyników prac z właścicielami i osobami odpowiedzialnymi za architekturę danych resortów i instytucji oraz poszczególne zasoby informacyjne państwa. Poinformował, że planowana jest publikacja wyników prac na portalu interoperacyjności.

W związku z realizacją celów dwóch ww. zadań Zespół AIP przygotował następujące dokumenty *Wizja Architektury Informacyjnej Państwa, Interoperacyjność systemów (Wizja AIP)* i *Zasady Zarządzania Architekturą Informacyjną Państwa (Model AIP[47])*.

---

[45] Zespół AIP to grupa kompetencyjna działająca w ramach resortu cyfryzacji, która w ścisłej współpracy z architektami innych instytucji. Zajmuje się modelowaniem architektury informacyjnej zgodnej z Programem Zintegrowanej Informatyzacji Państwa, zarówno w zakresie dokumentowania stanu istniejącego, systemów planowanych, jak i wizji dalszego rozwoju. Wynik prac zespołu jest na bieżąco przedstawiany Radzie Architektury, tak aby na podstawie wypracowanych koncepcji mogła ona przedkładać KRMC propozycje działań na rzecz spójnego, ustrukturyzowanego i zoptymalizowanego rozwoju środowiska systemów teleinformatycznych administracji publicznej.

[46] Komitet Rady Ministrów do spraw Cyfryzacji (dalej KRMC) organ pomocniczy Rady Ministrów i Prezesa Rady Ministrów powołany zarządzeniem Nr 48 Prezesa Rady Ministrów z dnia 12 kwietnia 2016 r. w sprawie Komitetu Rady Ministrów do spraw Cyfryzacji (M.P. z 2018 r. poz. 705, ze zm.).

[47] Model AIP (graficzno-tekstowy widok cyfrowego państwa), którego podstawowym zadaniem jest wspomaganie mechanizmu opiniowania i monitorowania projektów informatycznych

Efektem działania Zespołu AIP było opracowanie metody architektury danych państwa (warstwa semantyczna AIP), natomiast nadal prowadzone były prace nad rozwojem i dopasowaniem tej metody. Ponadto trwały prace nad opracowaniem architektury danych państwa w repozytorium AIP (identyfikacja, klasyfikacja i modelowanie kluczowych zasobów informacyjnych i rejestrów publicznych państwa, opracowanie koncepcyjnego modelu danych państwa, modeli kluczowych przepływów danych, opracowanie standardów i rekomendacji architektonicznych w obszarach kluczowych danych). Na podstawie analizy aktów prawnych zidentyfikowano i wstępnie zaklasyfikowano ponad tysiąc rejestrów publicznych, opracowano około 100 podstawowych modeli danych i rejestrów oraz szczegółowe modele i rekomendacje w obszarze danych 'Osoby fizycznej'.

Realizacja przez MC działania określonego w SOR pn. *Budowa kompetencji cyfrowych administracji, zarówno technicznych, jak i dotyczących praktycznego stosowania technologii cyfrowych*

Działanie pn. *Budowa kompetencji cyfrowych administracji, zarówno technicznych, jak i dotyczących praktycznego stosowania technologii cyfrowych*, wykonywane było poprzez realizację (w zakresie przypisanym MC) celu szczegółowego nr 3 PZIP, tj. *podniesienie poziomu kompetencji cyfrowych obywateli, specjalistów TIK oraz pracowników administracji publicznej*. W ramach działania:

- utworzono bazę wiedzy administracji z zakresu otwartości danych publicznych na portalu dane.gov.pl (https://dane.gov.pl/knowledgebase/multimedia-training), która obejmuje m.in. multimedialne materiały edukacyjne, standardy otwartości danych w wymiarach: prawnym, bezpieczeństwa, technicznym i API;
- następowała optymalizacja i rozwój Portalu gov.pl, w tym budowa platformy publikacji, integracja z innymi projektami, której efektem jest reorientacja administracji publicznej na usługi zorientowane na obywatela;
- przygotowano projekt Programu Rozwoju Kompetencji Cyfrowych (PRKC). PRKC to wieloletni program z perspektywą realizacji do 2030 r. Przewiduje on rozwój powszechnych kompetencji cyfrowych wśród obywateli, począwszy od etapu edukacji przedszkolnej i wczesnoszkolnej do wieku senioralnego. Wsparcie w ramach PRCK ma być kierowane do wszystkich, którzy będą chcieli podnosić swoje kompetencje cyfrowe, w tym do przedsiębiorców, pracowników gospodarki oraz urzędników, jak również ludzi utalentowanych cyfrowo, którzy zasilą w przyszłości zasób specjalistów ICT[48]. Równolegle w Programie przewidziano działania na rzecz integracji cyfrowej, służące likwidowaniu wykluczenia cyfrowego poprzez propagowanie i zwiększenie dostępności cyfrowych stron internetowych i aplikacji mobilnych dla osób z niepełnosprawnościami. W Programie znajdą się również inicjatywy mające na celu zwiększenie świadomości dotyczącej korzystania z technologii cyfrowych oraz propagowanie higieny cyfrowej. Dyrektor Generalny MC poinformował, że *opracowanie PRKC zostało zakończone*

w ramach prac KRMC, przez dostarczanie niezbędnej wiedzy Radzie Architektury IT i wsparcie w rozwiązywaniu istniejących problemów w interoperacyjności rejestrów publicznych i głównych systemów informatycznych państwa.

[48] ICT – z ang. *Information and communication technologies* – technologie informacyjno-komunikacyjne.

terminowo (w terminie do 31 grudnia 2019 r.). (...) Obecnie prace analityczne i konsultacje robocze koncentrują się wokół identyfikacji metody wdrażania całości PRKC, jak również jego działań oraz projektów w obliczu zmian będących skutkiem pandemii wirusa SARS-CoV-2, w tym m.in. planowane jest przeprowadzenie konsultacji (międzyresortowych i publicznych) w związku z perspektywą przyjęcia PRCK do realizacji w drodze Uchwały Rady Ministrów. Planowane przyjęcie programu to IV kwartał 2020 r.

Realizacja przez MC działania określonego w SOR pn. *Zastosowanie instrumentów analitycznych służących identyfikacji potrzeb obywateli w ramach e-administracji oraz wspieraniu działań podnoszących aktualność i wiarygodność danych znajdujących się w rejestrach państwowych*

Celem działania pn. *Zastosowanie instrumentów analitycznych służących identyfikacji potrzeb obywateli w ramach e-administracji oraz wspieraniu działań podnoszących aktualność i wiarygodność danych znajdujących się w rejestrach państwowych*, było *stałe podnoszenie kompletności danych w rejestrach wchodzących w skład SRP oraz implementacja w rejestrach zmian wynikających ze zmian legislacyjnych w przewidzianych prawem terminach.* W ramach działania do 30 czerwca 2020 r.:

- wprowadzono zmianę w ustawie o informatyzacji, która od 1 stycznia 2022 r. obliguje podmiot prowadzący rejestr publiczny przy użyciu systemów teleinformatycznych, do uprzedniej weryfikacji danych wprowadzanych po raz pierwszy do tego rejestru pod względem zgodności tych danych z danymi zgromadzonymi w rejestrze PESEL[49];
- w dniu 28 maja 2020 r. w życie wszedł przepis art. 48 ust. 3 ustawy o ewidencji ludności, zgodnie z którym na podstawie danych uzyskanych z rejestru PESEL za pomocą urządzeń teletransmisji danych, podmioty wymienione w ustawie i realizujące zadania publiczne niezwłocznie po ich uzyskaniu aktualizują dane w prowadzonych przez siebie rejestrach publicznych;
- w 2019 r. w ramach rejestru PESEL wdrożono usługę polegającą na zgłaszaniu niezgodności danych do właściwych organów;
- w 2018 r. rozszerzono zakres danych w PESEL i wprowadzono tzw. parentyzację tzn. jednoznaczne powiązanie rodzica z dzieckiem przez odwołanie do numeru PESEL;
- we współpracy z COI prowadzono projekt *Poprawy Jakości Danych w SRP*, w celu zidentyfikowania i analizy obszarów, które mogą zostać poprawione w sposób automatyczny np. uzupełnienie określonych danych;
- określono standardy technologiczne funkcjonowania systemu rejestrów państwowych i wymiany danych przetwarzanych w rejestrach publicznych utrzymywanych z wykorzystaniem systemu rejestrów państwowych;
- dla użytkowników uruchomiono platformę szkoleniową zawierającą instrukcję prawidłowej rejestracji danych w rejestrach państwowych.

[49] Art. 14 ust. 3 dodany przez art. 1 pkt 3 ustawy z dnia 16 października 2019 r. (Dz. U. z 2019 r. poz. 2294) zmieniającej ustawę z dniem 22 grudnia 2019 r., z tym że w zakresie dotyczącym rejestrów publicznych innych niż rejestr danych kontaktowych osób fizycznych wejdzie w życie z dniem 1 stycznia 2022 r.

5.2. Zapewnienie przez Centralny Ośrodek Informatyki funkcjonowania platformy ePUAP oraz profilu zaufanego

COI zapewnił utrzymanie i rozwój ePUAP oraz PZ jednak w realizacji zadania wystąpiły nieprawidłowości

W okresie poddanym kontroli COI zgodnie z umowami zawartymi z MC zapewnił utrzymanie i rozwój systemów ePUAP oraz PZ, jednak w realizacji tego zadania stwierdzono kilka nieprawidłowości.

Dla zapewnienia dostępności systemu na poziomie określonym w umowach z MC, COI zawarł umowy z usługodawcami zewnętrznymi i monitorował ich wykonanie. W razie niezapewnienia dostępności usług zewnętrznych na określonym poziomie COI naliczał kary umowne.

Dostępność systemów ePUAP i PZ utrzymywała się powyżej minimalnych progów określonych w umowach, tj. 98% dla ePUAP oraz 99% dla PZ. Według raportów utrzymania przekazywanych przez COI do MC wynosiła ona 100%. Kontrola NIK wykazała jednak, że zasady obliczania dostępności tych systemów określone w umowach na utrzymanie były nierzetelne, ponieważ przyjęto założenie, że dostępność tą zmniejszają jedynie ściśle określone incydenty krytyczne, które powodują niedostępność głównych funkcji systemu, natomiast incydenty o niższym priorytecie, które faktycznie utrudniały lub uniemożliwiały korzystanie z systemów przez użytkowników, nie miały wpływu na obniżenie raportowanego poziomu dostępności.

COI skutecznie monitorował działanie systemów ePUAP i PZ, reagując na pojawiające się awarie. Wsparcie techniczne dla użytkowników tych systemów zostało zorganizowane zgodnie ze współczesną praktyką w tym zakresie. Zaległości w obsłudze zgłoszeń wpływających od użytkowników tych systemów narastały w I połowie 2020 r., co spowodowane było zwiększonym wykorzystaniem tych platform przez obywateli i urzędy w związku ze stanem epidemii COVID-19. W COI podjęto odpowiednie działania zmierzające do poprawy tej sytuacji.

COI na zlecenie Ministerstwa Cyfryzacji rozwijał systemy ePUAP i PZ oraz podjął w tym zakresie współpracę z interesariuszami tych systemów. Realizowany przez COI proces zarządzania zmianami, od strony proceduralno-zarządczej był zorganizowany prawidłowo, w sposób typowy dla tego rodzaju procesów.

W COI podjęto działania w celu wdrożenia wymagań międzynarodowej normy z zakresu bezpieczeństwa informacji ISO/IEC 27001. Ponadto COI wdrożył procedury i zapewnił możliwość odtworzenia systemu w przypadku wystąpienia katastrofy.

Stwierdzone nieprawidłowości polegały m.in. na:

- **określeniu w umowach na utrzymanie systemów ePUAP oraz PZ nierzetelnego mechanizmu pomiaru jakości obsługi zgłoszeń problemów przez użytkowników, który nie uwzględniał wielkości przekroczenia wymaganego czasu obsługi, a jedynie sam fakt przekroczenia. Kontrola NIK wykazała, że w marcu 2020 r. odpowiednio 76% incydentów dotyczących PZ i 63% incydentów dotyczących ePUAP nie zostało nawet otwartych, a zaraportowana**

do MC skuteczność obsługi zgłoszeń dla systemu ePUAP wynosiła 93,6%, natomiast dla systemu PZ 96,2%;
- **określeniu w umowach na utrzymanie systemów ePUAP i PZ zbyt długich maksymalnych czasów obsługi poszczególnych kategorii incydentów, co może utrudnić korzystanie z tych systemów przez obywateli i urzędy;**
- **niepełnym wdrożeniu (do dnia zakończenia czynności kontrolnych) Systemu Zarządzania Bezpieczeństwem Informacji, co było niezgodne z § 20 ust. 1 i 3 rozporządzenia KRI;**
- **przeprowadzeniu przez COI niekompletnych testów bezpieczeństwa systemów ePUAP i PZ, co w ocenie NIK było działaniem nierzetelnym.**

Wprowadzenie

System ePUAP umożliwia podmiotom publicznym udostępnianie obywatelom e-usług na ogólnopolskiej platformie teleinformatycznej. Dostęp do ePUAP oraz e-usług możliwy jest m.in. z wykorzystaniem PZ, który zapewnia identyfikację elektroniczną użytkownika.

Na podstawie umowy nr 2/U/COI/MC/2016 zawartej 30 marca 2016 r. pomiędzy Ministrem Cyfryzacji oraz Centralnym Ośrodkiem Informatyki, COI jest odpowiedzialny za utrzymanie systemu ePUAP. W dniu 4 kwietnia 2019 r. MC zawarło z COI Aneks nr 4 do ww. umowy, zgodnie z którym okres jej obowiązywania został przedłużony do 4 kwietnia 2022 r. Na podstawie umowy zawartej 29 grudnia 2017 r. pomiędzy Ministrem Cyfryzacji oraz Centralnym Ośrodkiem Informatyki, COI do 30 grudnia 2020 r. jest odpowiedzialny za utrzymanie systemu PZ. W ww. umowach przewidziano także możliwość rozwoju tych systemów przez COI.

Serwis internetowy epuap.gov.pl

Na stronie www.epuap.gov.pl udostępniono dwie podstawowe metody wyszukiwania usługodawców (urzędów) i spraw załatwianych przez nich w formie e-usług. Zgodnie z instrukcją pn. *ePUAP Jak załatwić sprawę?*[50], pierwsza metoda polega na wyszukiwaniu spraw za pomocą wyszukiwarki zamieszczonej na stronie głównej ePUAP. Według drugiej metody wyszukiwanie urzędów możliwe jest z pomocą wyszukiwarki zamieszczonej w zakładce *Katalog spraw*, w której po odnalezieniu podmiotu właściwego miejscowo i rzeczowo oraz wyborze zakładki *Pokaż sprawy wybranego urzędu,* prezentowane są w sposób hierarchiczny najważniejsze kategorie i podkategorie zdarzeń, do których przyporządkowane zostały nazwy spraw, jakie użytkownik może zrealizować w wybranym przez siebie podmiocie. Inny sposób wyszukiwania urzędów, funkcjonujący w ramach drugiej metody wyszukiwania za pomocą zakładki *Katalog spraw* polega na wyborze opcji: *Inny podział spraw -> Klasyfikacja terytorialna* (dostępne inne opcje: *Alfabetyczna lista spraw oraz Inne klasyfikacje*), której wybór prezentuje usługi dostępne wyłącznie na terenie wybranej jednostki terytorialnej np. konkretnej gminy na terenie Rzeczypospolitej Polskiej. Wybranie jednej z usług świadczonych przez jednostki samorządu terytorialnego pozwala wyszukać urząd i sprawdzić, czy dana usługa jest przez niego realizowana.

[50] Dostępnej na stronie www.epuap.gov.pl w zakładce POMOC -> Załatwianie sprawy.

W celu weryfikacji działania drugiej metody wyszukiwania spraw według wybranego urzędu, poddano analizie według ww. instrukcji e-usługi udostępnione na stronie internetowej www.epuap.gov.pl przez 10 urzędów administracji publicznej[51]. Ustalono, że dla każdego z wybranych urzędów katalogi zawierały zarówno usługi świadczone przez te podmioty oraz inne usługi, które nie mogły być do tych urzędów przypisane, a adresatami tych usług były inne podmioty (np. ministerstwa).

Szczegółowe sprawdzenie możliwości załatwienia dwóch spraw[52] w sposób elektroniczny za pośrednictwem platformy ePUAP przypisanych do Urzędu Miejskiego w Sochaczewie wykazało, iż przypadku pierwszej sprawy wystąpił błąd formularza uniemożliwiający złożenie pisma, którego adresatem w rzeczywistości było Ministerstwo Cyfryzacji, a w przypadku drugiej sprawy wprawdzie była możliwość załatwienia sprawy w sposób elektroniczny, ale przez przekazanie informacji do nieistniejącego od ponad czterech i pół roku podmiotu tj. Ministerstwa Spraw Wewnętrznych[53]. Na podstawie analizy listy usług świadczonych przez UM w Sochaczewie na platformie ePUAP ustalono, że nie zostały opublikowane informacje dla części usług w zakresie nazwy organu właściwego do realizacji usługi, tj. wpisana jest informacja *Brak*[54], bądź zostały opublikowane informacje dotyczące nieistniejącego Ministerstwa Spraw Wewnętrznych[55] i Ministra Finansów, Inwestycji i Rozwoju[56] oraz wielokrotnie przy opisie usług występowało różne nazewnictwo organu właściwego do realizacji usługi przez jednostki samorządu terytorialnego, np. *Organ gminy*, w innym przypadku *Organ gminy (wójt, burmistrz, prezydent miasta)* lub *wójt, burmistrz, prezydent miasta*.

Dyrektorzy Pionu Operacji oraz Pionu Rozwoju COI wyjaśnili m.in., że zgodnie z art. 19d ustawy o informatyzacji, *podmioty udostępniające usługi na ePUAP zapewniają ich zgodność z przepisami stanowiącymi podstawę sporządzenia wzoru dokumentu elektronicznego oraz dokonują aktualizacji tych usług w katalogu usług. Oznacza to, że za informacje zawarte w usłudze oraz ich aktualność i zgodność z przepisami odpowiadają poszczególne podmioty udostępniające usługi. Jeżeli urząd opublikuje*

[51] Na podstawie sprawdzenia kategorii zdarzeń oraz usług świadczonych dla danej kategorii dla Urzędu Miasta (dalej: UM) w Sochaczewie, UM w Piastowie, UM w Hajnówce, UM w Augustowie, UM w Knurowie, UM w Wolsztynie, UM w Oławie, UM w Zgorzelcu, UM w Policach oraz Gminie Knurów i Gminie Koluszki.

[52] Pierwszej pn. Przekazanie informacji o udostępnionym przez podmiot publiczny adresie Elektronicznej Skrzynki Podawczej należącej do kategorii Udostępnianie usług -> Udostępnianie przez podmiot publiczny adresu Elektronicznej Skrzynki Podawczej oraz drugiej pn. Udostępnianie danych z rejestru PESEL i rejestru mieszkańców za pomocą urządzeń teletransmisji danych należącej do kategorii Sprawy obywatelskie -> Ogólne sprawy urzędowe.

[53] Istniało do dnia 15 listopada 2015 r. Na podstawie rozporządzenia Rady Ministrów z dnia 20 listopada 2015 r. w sprawie utworzenia Ministerstwa Spraw Wewnętrznych i Administracji (Dz. U. z 2015 r. poz. 1946), od 16 listopada 2015 r. MSW zostało przekształcone w Ministerstwo Spraw Wewnętrznych i Administracji.

[54] Np. usługa Sporządzenie aktu zgonu należąca do kategorii Sprawy obywatelskie ->Zgłaszanie zmian w aktach stanu cywilnego.

[55] Np. usługa Udostępnianie danych z Rejestru Dowodów Osobistych w trybie ograniczonej teletransmisji danych należąca do kategorii Sprawy obywatelskie -> Ogólne sprawy urzędowe.

[56] Np. usługa Informacja o prognozowanych przychodach firmy audytorskiej dla Komisji Nadzoru Audytowego (KNA-INF) należąca do kategorii Najnowsze usługi -> Najnowsze usługi centralne.

np. nieaktualne dane o swoim urzędzie, np. wpisał nazwę urzędu, takie dane będą również wyświetlały się w katalogu usług na ePUAP. W zakresie błędu, który wystąpił w tracie wywołania usługi (...) system ePUAP działał w tym zakresie prawidłowo. Przedmiotowy błąd dotyczył wyłącznie usługi, która została opublikowana w katalogu usług, za której działanie odpowiada podmiot ją umieszczający (...).

Dyrektor Departamentu Produkcji Oprogramowania COI wyjaśnił, iż weryfikacja listy e-usług świadczonych przez Urzędy nie jest przedmiotem umowy pomiędzy COI, a MC, natomiast COI *mając na uwadze prawidłowe funkcjonowanie systemu realizuje, w ramach wsparcia MC, zadania polegające na manualnej weryfikacji opisów każdej z usług zgłoszonych przez podmioty realizujące zadania publiczne (Urzędy) przed ich publikacją. Weryfikacji podlega kompletność opisu usługi w poszczególnych polach formularza. W przypadku stwierdzenia błędów usługa jest odrzucana przez Centralny Ośrodek Informatyki z powiadomieniem wnioskującego o przyczynie odrzucenia. Następnie proces publikacji opisu usługi rozpoczyna się od początku.*

NIK zauważa, że wprawdzie COI przejął od Centrum Cyfrowej Administracji w 2016 r. do eksploatacji funkcjonujący już system, jednak jako podmiot utrzymujący system powinien informować właściciela systemu (MC) o konieczności dokonania zmian w ramach prac rozwojowych, które pozwoliłyby na wyeliminowanie ww. problemów.

Ponadto zdaniem NIK, COI we współpracy z właścicielem systemu powinien dokonać modyfikacji zastosowanego mechanizmu filtrowania (wyszukiwania) poprzez jego rozbudowanie o możliwość wyboru przez użytkownika usług lokalnych lub centralnych, które mogą być załatwione przez dany podmiot, ujednolicić nazewnictwo adresatów usług za pomocą słowników lub powiązać je ze źródłami danych zewnętrznych, a także wdrożyć rozwiązania nadzorcze w celu niezwłocznego aktualizowania udostępnionych usług przez ich właścicieli. Takie działanie ma na celu zapewnienie prawidłowości wyświetlanych informacji.

Zapewnienie przez COI sprawnego działania ePUAP oraz PZ

W umowach na utrzymanie systemów ePUAP i PZ dostępność SLA określono na poziomie 98% w odniesieniu do systemu ePUAP oraz 99% w odniesieniu do systemu PZ. Przyjęcie takich wartości powoduje możliwość zaistnienia całkowitej niedostępności każdej z usług przez 7,3 dnia w ciągu roku dla systemu ePUAP oraz przez 3,6 dnia dla systemu PZ.

W opinii NIK, systemy ePUAP i PZ, z uwagi na istotne znaczenie dla obywateli i dla funkcjonowania administracji publicznej, powinny mieć gwarantowaną w umowach dostępność o wartości zbliżonej do bankowych systemów informatycznych, tj. 99,9%, co jest szczególnie ważne w sytuacji epidemii COVID-19.

Zgodnie z zawartymi umowami na utrzymanie systemów ePUAP i PZ, COI był zobowiązany do przekazywania MC miesięcznych raportów dotyczących poziomu świadczonych usług utrzymania. Według raportów za okres lipiec

2019 r.–czerwiec 2020 r. dostępność systemów ePUAP oraz PZ w każdym miesiącu tego okresu wynosiła 100%. Dostępność ta była wyznaczana jako iloraz sumy czasów trwania incydentów krytycznych w miesiącu do łącznego czasu wymaganej dostępności systemu w tym czasie.

Analizie poddano zarejestrowane przez COI incydenty krytyczne i pilne od lipca 2019 r. do czerwca 2020 r. oraz incydenty standardowe, które wystąpiły w dniu 22 stycznia 2020 r., kiedy to nastąpiła awaria serwera baz danych w jednym z ośrodków przetwarzania. Ustalono, że w badanym okresie incydentów krytycznych w ogóle w COI nie zarejestrowano (ostatni taki incydent miał miejsce 14 czerwca 2018 r.). W listopadzie i grudniu 2019 r. wystąpiły natomiast dwa incydenty pilne dotyczące awarii bramek SMS obsługujących system ePUAP[57]. Dla systemu PZ incydentów o priorytecie innym niż standardowy nie odnotowano. Według wyjaśnień Dyrektora Pionu Operacji COI, pomimo awarii serwera 22 stycznia 2020 r., system ePUAP był dostępny, natomiast część użytkowników postrzegała go jako niedostępny.

NIK zauważa, że incydent sklasyfikowany jako mniej istotny – standardowy lub pilny – może uniemożliwić sprawne korzystanie z systemu przez użytkowników, natomiast zgodnie z umowami utrzymania nie będzie on wpływał na raportowaną dostępność systemów.

Z ustaleń kontroli NIK wynika, że określony w umowach na utrzymanie systemów ePUAP i PZ i stosowany w przekazywanych przez COI do MC raportach sposób obliczania dostępności tych systemów nie uwzględniał ich rzeczywistej dostępności, która dla użytkowników jest niższa niż raportowana dostępność na poziomie 100%. Kontrola wykazała, że zgodnie z umowami na utrzymanie systemów raportowany czas ich dostępności może zmniejszyć jedynie zaistnienie incydentu krytycznego. **Przyjęcie w umowach wąskiej definicji incydentu krytycznego powoduje, że awaria uzasadniająca sklasyfikowanie go jako krytyczny (a co za tym idzie obniżenie raportowanego poziomu SLA) jest trudna do zaistnienia. W umowach na utrzymanie systemów ePUAP i PZ ustalono maksymalne czasy obsługi poszczególnych kategorii zgłoszeń, które są zbyt długie, gdyż mogą utrudnić korzystanie z tych systemów przez obywateli i urzędy.** I tak, dla systemu ePUAP maksymalny czas na obsługę incydentu krytycznego w okresie od 30 marca 2016 r. do 4 kwietnia 2019 r. wynosił trzy dni robocze (od tej daty – jeden dzień roboczy). Dla porównania czas obsługi incydentów krytycznych dla systemu PZ wynosił do 11 godzin. Natomiast czas obsługi incydentów pilnych zarówno dla systemu ePUAP, jak i PZ wynosił 10 dni roboczych, a incydentów standardowych – 20 dni roboczych. Dyrektor Pionu Operacji COI wyjaśnił, że *czasy obsługi zgłoszeń zostały ustalone w wyniku uzgodnień pomiędzy stronami umowy na podstawie doświadczeń w utrzymaniu systemów. Należy podkreślić, iż są to graniczne czasy obsługi zgłoszeń, wynikające między innymi ze specyfiki niektórych incydentów, wymagających długotrwałych działań naprawczych. W przypadku incydentów krytycznych Centralny Ośrodek Informatyki podej-*

[57] Awaria bramek SMS powoduje brak możliwości dokonania autoryzacji czynności użytkownika.

muje działania w trybie 24/7 w celu jak najszybszego usunięcia incydentu, aby jak najszybciej zarządzić sytuacją kryzysową.

Sprawne działanie i dostępność systemów ePUAP i PZ na poziomie ustalonym w umowach utrzymaniowych zależy w dużej mierze od jakości 11 usług i dostaw świadczonych na rzecz COI przez usługodawców zewnętrznych, które obejmowały dostawę licencji w zakresie oprogramowania, dostawę sprzętu, a także świadczenie usług dostępu do Internetu, wysyłania krótkich wiadomości tekstowych oraz usług serwisu, wsparcia technicznego sprzętu i oprogramowania. W zawartych przez COI umowach dotyczących świadczenia usług telekomunikacyjnych określono zarówno maksymalne czasy usunięcia awarii, jak i wymagany poziom dostępności danej usługi, przy czym dostępność tą określono na poziomie 99,5%. W pozostałych umowach z usługodawcami zewnętrznymi określono czas na usunięcie awarii, natomiast nie uregulowano poziomu dostępności.

Umowy, w których określono wymaganą dostępność usług zewnętrznych zawierają zobowiązanie usługodawcy do przekazywania COI miesięcznych raportów o poziomie ich świadczenia. Raporty te były przekazywane do COI przez podmioty dostarczające usługi na rzecz ePUAP oraz PZ. Zawierały one informacje o dokonanych przez COI zgłoszeniach a także osiągniętych w danym miesiącu poziomach dostępności. Ich analizą i rozliczaniem zajmował się Zespół Zarządzania Poziomem Usług w COI. Incydenty, czy awarie dotyczące korzystania z usług dostawców zewnętrznych były rejestrowane w systemie ITSM Atmosfera i zgłaszane usługodawcom, a po ich rozwiązaniu rejestrowany był moment zamknięcia.

Analizie poddano sprawność działania usług świadczonych przez podmioty zewnętrzne w okresie od lipca 2019 r. do czerwca 2020 r. Ustalono, że istotne awarie dotyczyły jedynie usługi wysyłania powiadomień SMS, które w tym okresie miały miejsce jedenastokrotnie, w tym trzykrotnie doprowadziły do przekroczenia określonych w umowach parametrów dostępności SLA. W takim przypadku COI każdorazowo naliczał usługodawcy kary umowne.

NIK zauważa, że przyjęty poziom dostępności usług telekomunikacyjnych odbiega od poziomów rynkowych dla branży telekomunikacyjnej, które zazwyczaj wynoszą 99,9%. Ponadto dla zapewnienia sprawnego działania systemów ePUAP i PZ należy dążyć do umownego uregulowania z wykonawcami parametrów dostępności świadczonych przez nich usług.

Należy podkreślić, iż pomimo dotychczasowego sprawnego działania tych usług może zaistnieć sytuacja, w której wprawdzie awarie będą usuwane terminowo, jednak dostępność usług zewnętrznych spadnie poniżej oczekiwanego przez użytkowników poziomu umożliwiającego zapewnienie sprawnego działania ePUAP i PZ.

Infrastruktura teleinformatyczna, w oparciu o którą funkcjonują systemy ePUAP i PZ, znajdowała się w podstawowym i zapasowym ośrodku przetwarzania danych. Serwerownie te są własnością Skarbu Państwa i na podstawie porozumienia pomiędzy Komendantem Głównym Policji i Ministrem Spraw Wewnętrznych z 5 lutego 2014 r. zostały oddane w uży-

czenie Ministerstwu Spraw Wewnętrznych. Na podstawie umowy użyczenia z 22 lutego 2018 r. pomiędzy Ministerstwem Spraw Wewnętrznych i Administracji, a Ministerstwem Cyfryzacji serwerownie te zostały oddane MC w nieodpłatne używanie na czas nieoznaczony. Umowa ta nie zawierała postanowień dotyczących wymaganego poziomu usług w zakresie zasilania, chłodzenia czy ochrony serwerowni przez użyczającego.

Zdaniem NIK, brak określenia takich parametrów może negatywnie wpływać na zapewnienie sprawnego działania systemów ePUAP i PZ. Należy jednak mieć na względzie, że COI nie było stroną ww. umowy użyczenia i tym samym odpowiada jedynie za infrastrukturę teleinformatyczną znajdującą się w serwerowni oraz za prawidłowe działanie systemów ePUAP i PZ. COI powinno jednak dążyć do umownego określenia parametrów, co pozwoli na zapewnienie dostępności tych systemów na najwyższym możliwym poziomie.

Podstawowa serwerownia systemów ePUAP i PZ posiada wszystkie typowe zabezpieczenia fizyczne i lokalowe, stosowane w tego typu obiektach. Zainstalowano m.in. system kontroli dostępu i włamania, system przeciwpożarowy, system kontroli parametrów środowiskowych serwerowni (wilgotności, temperatury) oraz system monitoringu. W pomieszczeniu tym zainstalowany jest wyłącznie sprzęt teleinformatyczny (szafy, serwery, podłoga techniczna z osprzętem) i nie przebywają tam na stałe pracownicy. Serwerownia ta wyposażona jest w system baterii UPS i agregaty prądotwórcze w celu podtrzymania dostaw energii elektrycznej dla infrastruktury.

Wsparcie techniczne dla użytkowników ePUAP i PZ

Wsparcie techniczne dla użytkowników systemów ePUAP i PZ zostało zorganizowane przez COI w ramach tzw. trzech linii wsparcia. Pierwszą linię stanowili pracownicy Zespołu Service Desk, do których zadań należała rejestracja i obsługa zgłoszeń napływających od użytkowników, a w razie braku możliwości rozwiązania problemu jego przekazanie do kolejnych linii wsparcia.

Drugą linię wsparcia stanowili pracownicy Zespołu Administrowania Systemami i Zespołu Infrastruktury, a także Zespołu Bezpieczeństwa Teleinformatycznego i Zespołu Zarządzania Wydaniem i Konfiguracją.

Jeżeli rozwiązanie problemu wymagało dokonania zmian w oprogramowaniu systemów zgłoszenie było przekazywane do trzeciej linii wsparcia, która była obsługiwana przez programistów, testerów i ekspertów Zespołu Rozwoju Usług Cyfrowych oraz Zespołu Integracji i Testów.

Użytkownicy systemów ePUAP i PZ mogli zgłaszać problemy i pytania poprzez pocztę elektroniczną, formularz kontaktowy na stronie internetowej, a także telefonicznie. Zgodnie z umowami utrzymaniowymi ePUAP i PZ zgłoszenia telefoniczne były przyjmowane od użytkowników w dni robocze w godzinach 8:00–17:00. Zgłoszenia były rozwiązywane przez pierwszą linię wsparcia w godzinach 8:00–16:00. Poza tymi godzinami działanie systemu było na bieżąco, całodobowo monitorowane przez Sekcję COI-Houston.

Potwierdzenie zakończenia obsługi zgłoszenia było realizowane za pomocą poczty elektronicznej. Ocena satysfakcji zgłaszającego ze sposobu rozwią-

zania problemu, może być dokonana za pomocą tych samych kanałów komunikacji: telefonicznie, mailowo lub poprzez formularz zgłoszeniowy, gdzie jedną z kategorii zgłoszenia jest opinia.

Na podstawie umów utrzymaniowych, COI sporządzał i przekazywał do MC miesięczne raporty dotyczące utrzymania systemów ePUAP i PZ, które zawierały m.in. informacje na temat liczby wszystkich incydentów (w tym z przekroczonym terminem obsługi), a także wykaz wszystkich zgłoszeń. **Ustalono, że COI przyjęło nierzetelny mechanizm pomiaru jakości obsługi zgłoszeń.** Na potrzeby wyliczenia liczby zgłoszeń obsłużonych w danym miesiącu terminowo COI kwalifikowało jedynie zgłoszenia zakończone w danym miesiącu, przy czym nie uwzględniano wielkości przekroczenia wymaganego czasu obsługi, a jedynie sam fakt przekroczenia. W efekcie przyjęcia takich założeń zamykanie przez COI incydentów opóźnionych w kolejnych miesiącach zmniejsza raportowaną skuteczność obsługi zgłoszeń, wobec czego COI nie ma motywacji do ich zamykania po przekroczeniu czasu na ich obsługę. W związku z powyższym **dane zaprezentowane w raportach utrzymania systemów ePUAP i PZ, dotyczące skuteczności obsługi zgłoszeń przez COI w danym miesiącu nie odzwierciedlały rzeczywistości.** Pomimo, iż np. w marcu 2020 r. odpowiednio 76% incydentów dotyczących PZ i 63% incydentów dotyczących ePUAP nie została nawet otwarta, zaraportowana do MC skuteczność obsługi zgłoszeń dla ePUAP wynosiła w marcu 93,6%, a w kwietniu 96,9%, natomiast dla PZ wyniosła odpowiednio 96,2% i 95,9%.

NIK zwraca uwagę, że umowy utrzymaniowe, wbrew praktyce rynkowej, nie określają wymaganych czasów reakcji na zgłoszenie, tj. czasu, jaki może upłynąć od zarejestrowania zgłoszenia w systemie do rozpoczęcia jego obsługi.

Dyrektor Pionu Operacji COI wyjaśnił, że *sposób rozliczania czasu obsługi zgłoszeń i ich raportowania wynika z umów utrzymaniowych na powierzone systemy. Umowy te zostały uzgodnione i podpisane przez Ministerstwo Cyfryzacji i Centralny Ośrodek Informatyki. W raporcie uwzględnia się zgłoszenia, których obsługa została zakończona w danym miesiącu. Raport prezentuje zgłoszenia, z podziałem na zgłoszenia zrealizowane i niezrealizowane zgodnie z SLA. (…) Jeśli dojdzie do przekroczenia SLA incydentu to zostanie ono zaraportowane w miesiącu, w którym zakończy się jego obsługa. W momencie raportowania pracownik nie jest w stanie stwierdzić jak duże przekroczenie zostanie odnotowane na danym incydencie, kiedy faktycznie nastąpi jego realizacja. Model raportowania przyjęty przez COI jest zgodny z aktualnymi trendami rynkowymi. Model ten stawia na pierwszym miejscu percepcję użytkownika końcowego, dla którego kluczowa jest realizacji incydentu w terminie, a nie średni czas przekroczenia SLA. Należy podkreślić, że wskazany (…) okres, tj. marzec–czerwiec 2020 r., ze względu na sytuację epidemiczną w kraju jest wybitnie niereprezentatywny. W okresie tym liczba zgłoszeń i połączeń telefonicznych była kilka razy wyższa niż w analogicznym okresie w roku 2019. Jednocześnie Service Desk realizował dodatkowe zadania zlecone przez Ministra Cyfryzacji (…).*

NIK zauważa, że przy wyliczeniach dostępności systemów uwzględnia się jedynie incydenty, których obsługa zakończyła się w danym miesiącu rozliczeniowym, co również ma wpływ na rzetelność określenia dostępności.

Dyrektor Pionu Operacji COI wyjaśnił, że te kwestie wynikają z umów podpisanych z MC. (...)Ponadto wyjaśnił, że *incydenty krytyczne powodują faktyczną niedostępność systemu lub jego głównych usług. (...) awaria bramki SMS może być zaklasyfikowana jako incydent krytyczny, bądź pilny. Stosowana w systemie ePUAP i PZ bramka SMS wykorzystuje usługi dwóch niezależnych operatorów. Jeśli awaria bramki SMS dotyczy jednego z operatorów nadal zachowana jest ciągłość usługi a incydent uznaje się jako pilny. Incydent krytyczny wystąpi wówczas, gdy dotyczy całkowitej niedostępności bramki SMS u obu operatorów. (...) zgodnie z umową utrzymaniową systemu PZ za incydent krytyczny uznaje się nieprawidłowe działanie systemu w środowisku produkcyjnym powodujący całkowity brak możliwości korzystania z głównych funkcji systemu. Główne funkcje systemu są wyszczególnione i opisane w załączniku numer 8 umowy utrzymaniowej, dzięki czemu strony umowy nie mają wątpliwości co do prawidłowej klasyfikacji danego incydentu. Wszystkie incydenty dotyczące głównych funkcji systemu, powodujące ich całkowitą niedostępność, uznawane są za incydenty krytyczne. (...) przyjęte zapisy służą zapewnieniu rozliczalności danej usługi. W raportach miesięcznych uwzględniane są incydenty, których obsługa została zakończona w danym okresie rozliczeniowym i których parametry obsługi można umieścić w raporcie. Incydenty, których obsługa nie została zakończona i nie znamy na moment końca okresu rozliczeniowego terminu ich zakończenia, są rozliczane w kolejnym okresie. Zamknięcie uniemożliwia ponowne otwarcie danego incydentu co pozwala na uniknięcie ryzyka związanego z powielaniem tych samych incydentów w kolejnych okresach i ich rozliczalność.*

NIK nie kwestionuje, że sposób obliczania dostępności systemów wynika z umów z MC i został tam szczegółowo opisany. Zdaniem NIK, przyjęty w tych umowach sposób obliczania dostępności systemu nie odzwierciedla jednak w pełni rzeczywistości.

Działania COI w I połowie 2020 r, w tym w czasie epidemii COVID-19

Kontrola wykazała, że w I połowie 2020 r. nastąpił gwałtowny wzrost liczby zgłoszeń problemów przez użytkowników dla obu systemów, który spowodował, że w każdym miesiącu pozostawały znaczne ilości zgłoszeń nieobsłużonych[58]. I tak, w okresie tym, w odniesieniu do systemu ePUAP, średnia liczba zgłoszeń nieobsłużonych w miesiącu wyniosła 8406[59], natomiast w odniesieniu do systemu PZ-6895[60]. Stanowi to wzrost średniomiesięcznej liczby nieobsłużonych zgłoszeń w stosunku do drugiej połowy 2019 r. odpowiednio o 557,5% w odniesieniu do systemu ePUAP

[58] W okresie lipiec 2019 r. – czerwiec 2020 r. do Zespołu Service Desk wpłynęło 126 007 zgłoszeń dotyczących systemu ePUAP (od 7091 w listopadzie 2019 r. do 18 216 w kwietniu 2020 r., średnio 10 501 zgłoszeń miesięcznie) oraz 100 120 zgłoszeń dotyczących systemu PZ (od 4814 w sierpniu 2019 r. do 15 007 w marcu 2020 r., średnio 8343 zgłoszeń miesięcznie).

[59] 2034 nieobsłużone zgłoszenia w styczniu, 2952 w lutym, 9046 w marcu, 17 027 w kwietniu, 10 200 w maju oraz 9175 w czerwcu.

[60] 3601 nieobsłużonych zgłoszeń w styczniu, 4472 w lutym, 12 526 w marcu, 8775 w kwietniu, 4780 w maju oraz 7218 w czerwcu.

i 613,6% w odniesieniu do systemu PZ. Dyrektor Pionu Operacji COI wyjaśnił, że stan ten wynikał z rozprzestrzeniania się w pierwszej połowie 2020 r. epidemii COVID-19 i związanym z tym zwiększonym zainteresowaniem obywateli e-usługami oraz zobowiązaniem COI do zaangażowania pracowników na rzecz podmiotów zewnętrznych (np. Głównego Inspektora Sanitarnego, Narodowego Funduszu Zdrowia, czy Sejmu RP).

Analiza treści zgłoszeń problemów wykazała ich niewielką powtarzalność. Najczęściej zgłaszane problemy dotyczyły:

- problemów z komponentem kryptograficznym, instalowanym lokalnie na komputerach i obsługiwanym w różnych przeglądarkach internetowych w całym kraju, (listopad 2019 r.–czerwiec 2020 r.);
- problemów z potwierdzeniem tożsamości za pośrednictwem systemu teleinformatycznego jednego z banków (kwiecień – czerwiec 2020 r.);
- błędów w działaniu systemu, które zwykle dotyczą pojedynczych użytkowników (wynikające np. z krótkotrwałego zawieszenia serwera aplikacyjnego)[61];
- problemów z logowaniem, spowodowanych brakiem danych do logowania (identyfikator i hasło).

Pozostałe zgłoszenia dotyczyły problemów w użytkowaniu systemów, które wynikały zarówno z ich wadliwego działania, jak i z niewiedzy użytkowników.

Poza rejestrowaniem i obsługą zgłoszeń o powtarzalnym charakterze COI podejmował działania zmierzające do ich trwałego wyeliminowania (np. umieszczenie na stronie internetowej COI instrukcji posługiwania się komponentem kryptograficznym, usuwanie usterek, zgłaszanie niesprawności bramek SMS, czy publikowanie i aktualizowanie listy najczęściej zadawanych pytań).

Według stanu na dzień 17 czerwca 2020 r. nad utrzymaniem systemów ePUAP i PZ pracowało w COI łącznie 112 osób (w tym: 33 osoby w pierwszej linii wsparcia). Porównanie liczby zgłoszeń wpływających i obsłużonych w danym miesiącu, a także dostępnych w COI zasobów kadrowych zaangażowanych w utrzymanie systemów ePUAP i PZ, w szczególności do obsługi zgłoszeń wskazuje, że były one wystarczające do końca 2019 r.

Narastające od początku 2020 r. zaległości w zakresie obsługi napływających zgłoszeń wymagały podjęcia przez COI działań zmierzających do ich likwidacji. Dyrektor COI wyjaśnił, że od 13 marca 2020 r. wszyscy pracownicy Zespołu Service Desk realizowali na rzecz podmiotów zewnętrznych dodatkowe zadania zlecone przez Ministra Cyfryzacji mające na celu minimalizację skutków pandemii COVID-19. Ponadto wyjaśnił, że COI (…) *podjął niezwłoczne działania, których celem było rozładowanie kolejki zgłoszeń i skrócenia czasu ich obsługi. Do Service Desk zostało przesuniętych 70 pracowników z innych zespołów. Jednocześnie uruchomiony został proces rekrutacji.* (…) **W opinii NIK, COI podjął odpowiednie działania w celu ograniczenia zaległości w obsłudze zgłoszeń użytkowników.**

Monitorowanie działania ePUAP i PZ

Monitorowaniem działania systemów ePUAP i PZ zajmuje się w COI Zespół COI-Houston funkcjonujący w trybie 24 godziny na dobę, przez siedem dni

[61] Sygnalizowanych np. jako External server error, Błąd 500.

w tygodniu. Wykorzystuje on w tym celu specjalistyczne narzędzia, które służą do bieżącego monitorowania zajętości infrastruktury systemów ePAUP i PZ. Monitorowaniu podlegają parametry obciążenia łącz w centrach danych (zarówno ruchu wchodzącego, jak i wychodzącego), a także użycia procesora, pamięci operacyjnej i dysków do trwałego przechowywania danych dla serwerów aplikacyjnych i bazodanowych. Pomiary parametrów wykonywane są punktowo, co 5 minut. W przypadku wystąpienia awarii zespół COI-Houston podejmował działania mające na celu jej usunięcie.

COI sporządzał i przekazywał do MC miesięczne raporty dotyczące obciążenia infrastruktury. Według raportu za maj 2020 r. stopień wykorzystania przestrzeni dyskowej systemów wynosił 55% w przypadku serwerów aplikacyjnych i 64% w przypadku serwerów bazodanowych.

Zdaniem NIK, takie wartości są typowe dla systemu znajdującego się w fazie produkcyjnej i pozostawiają bezpieczny margines wolnego miejsca, umożliwiający rozszerzenie dostępnych zasobów w razie potrzeby.

Rozwój systemów ePUAP i PZ oraz wprowadzanie zmian w oprogramowaniu

Możliwość zmian rozwojowych ePUAP i PZ została przewidziana w umowach utrzymaniowych tych systemów. W ramach określonego w tych umowach budżetu (45 300,0 tys. zł w umowie dotyczącej ePUAP[62] i 6696,4 tys. zł w umowie dotyczącej PZ[63]) MC mogło udzielać COI zleceń dodatkowych. W okresie obowiązywania tych umów MC udzieliło COI 17 zleceń rozwojowych dotyczących ePUAP oraz 17 zleceń rozwojowych dotyczących PZ. Prace rozwojowe dotyczące systemów były także realizowane w oparciu o umowę dotyczącą budowy Krajowego Węzła Identyfikacji Elektronicznej[64]. W związku z realizacją ww. zleceń rozwojowych, COI poniósł w latach 2017–2020 wydatki głównie na usługi obce[65], w łącznej wysokości:

- 1805,1 tys. zł w ramach prac rozwojowych ePUAP,
- 1209,6 tys. zł w ramach prac rozwojowych PZ,
- 14,6 tys. zł w ramach budowy Węzła Krajowego.

Prace rozwojowe systemu ePUAP dotyczyły m.in. wsparcia algorytmu kryptograficznego SHA-2, realizacji nowych usług, integracji ePUAP z innymi systemami i rejestrami. Natomiast rozwój PZ dotyczył m.in. prac nad podpisem PZ dla pliku JPK_VAT, stworzenia podpisu eDowodu w systemie PZ oraz automatycznej aktualizacji danych w bazie systemu PZ na podstawie zmian w rejestrze PESEL.

[62] Jest to górna granica zobowiązań MC z tytułu realizacji całej umowy, obejmującej również utrzymanie ePUAP, a także SSDIP, Strony Głównej BIP i Publikatora Aktów Prawnych.

[63] Ze środków tych MC mogło zlecać COI również zakup zewnętrznych usług, niezbędnych w procesie utrzymania systemów.

[64] Projekt realizowany przez MC, który ma ułatwić korzystanie z usług elektronicznych poprzez utworzenie jednego uniwersalnego loginu i bezpiecznego zestawu haseł.

[65] Usługi obce w tym Body Leasing, Delegacje pracowników Centralnego Ośrodka Informatyki oraz odsprzedaż sprzętu i licencji. Wydatki nie obejmują kosztów związanych z wynagrodzeniem pracowników COI, pochodnych na ZUS i ZFŚS, kosztów Amortyzacji, oraz kosztów pośrednich w tym m.in. opłat eksploatacyjnych, kosztów lokalizacji, usług pocztowych, użytkowania i eksploatacji części wspólnych itp.

Organizatorem współpracy z kluczowymi interesariuszami[66] w ramach prac nad rozwojem ePUAP oraz PZ w zakresie usług elektronicznych świadczonych za pośrednictwem tych systemów jest MC. COI brał udział w ww. pracach w charakterze wykonawcy oraz doradcy technologicznego MC. Przedstawiciele interesariuszy brali udział w posiedzeniach Komitetu Sterującego projektu pn. *Budowa Węzła Krajowego*, w pracach merytorycznych, a także w testach integracyjnych. Zadania realizowane przez COI z udziałem interesariuszy w zakresie rozwoju ePUAP dotyczyły głównie zmiany stosowanego w tym systemie algorytmu SHA-1 na SHA-2[67] i polegały na:

- koordynacji akcji kontaktu telefonicznego z wszystkimi potencjalnymi podmiotami na które mogła mieć wpływ zmiana algorytmu SHA-1 na SHA-2 (około 3 tys. interesariuszy),
- prowadzenia warsztatów zorganizowanych przez MC dla dostawców usług i dostawców tożsamości, którzy powinni dostosować własne systemy do algorytmu SHA-2,
- bezpośredniego wsparcia w siedzibie interesariusza (Centrala ZUS) w związku z wdrożeniem nowej aplikacji dla wykonania akcji podpisu kwalifikowanego,
- koordynacji testów integracyjnych wraz z obsługą zgłoszeń interesariuszy dotyczących udziału w testach wraz z wyznaczeniem koordynatorów na wdrożenie produkcyjne.

Interesariuszom na stronie głównej ePUAP[68] udostępniane były bieżące informacje dotyczące ePUAP i PZ, które publikowane są m.in. w sekcji *Aktualności* oraz instrukcje i podręczniki, a w sekcji *Pomoc* odpowiedzi na najczęściej zadawane pytania, dostępne niezależnie dla obywatela i urzędnika.

Zagadnienia dotyczące dokonywania zmian w wytworzonym oprogramowaniu zostały określone w następujących dokumentach COI:

– *Procedura Zarządzania Wydaniami*, w której uregulowano zarządzanie wydaniami nowych wersji oprogramowania od strony formalnej oraz organizacyjnej;
– *Procedura Zarządzania Wdrożeniami*, w której zdefiniowano zasady wdrażania zmian o dużym zakresie i uregulowano wytyczne na temat zaplanowania harmonogramu wdrożenia oraz sposobu jego realizacji.

Zgodnie z ww. procedurami, za zarządzanie wydaniami i wdrożeniami w COI odpowiada Rada ds. Zmian. Każda zmiana posiada przypisanego Właściciela Zmiany, tj. osobę inicjującą zmianę, która opracowuje dokument RFC[69]. Dokumentem, który całościowo opisuje dokonaną zmianę jest Karta

[66] Kluczowi interesariusze w ePUAP i PZ to m.in.: banki jako dostawcy tożsamości, dostawcy usług – podmioty publiczne posiadające uwierzytelnione konto na ePUAP w tym j.s.t., które wykorzystują ePUAP do przygotowywania i udostępniania własnych usług oraz wykorzystują PZ jako środek uwierzytelniający w celu świadczenia usług we własnych systemach, jednostki administracji publicznej korzystające z systemów ePUAP i PZ, które zgłaszają błędy, problemy, wnioski i pytania poprzez Service Desk COI.

[67] Zmiana dotyczyła również systemu PZ.

[68] Pod adresem: www.epuap.gov.pl.

[69] Ang. *Request for Comments.*

Wydania. Przed dokonaniem wdrożenia określany jest plan komunikacji z interesariuszami wdrożenia. W przypadku wdrożeń obarczonych dużym ryzykiem niepowodzenia powołuje się specjalny zespół i przygotowuje się plany na wypadek sytuacji kryzysowej. O ostatecznym wyniku działań wdrożeniowych przesądza wydanie decyzji przez osobę koordynującą wdrożenie (zazwyczaj przez Dyrektora COI) na podstawie rekomendacji zespołu realizującego wdrożenie.

Działania COI w zakresie procesu wytwarzania oprogramowania regulują:

- *Zasady wytwarzania oprogramowania w COI,* definiujące wprowadzenie nowego wprowadzania nowego kodu do wdrożenia*;*
- *Opis narzędzi stosowanych dla zapewnienia ciągłości procesu wytwórczego oprogramowania,* dotyczący narzędzi używanych przez COI, które służą do realizacji tzw. ciągłej integracji;
- *Procedura zapewniania bezpieczeństwa w zarządzaniu zmianą*, określająca proces konsultacji z Departamentem Cyberbezpieczeństwa na etapie przygotowywania, implementacji i wdrażania zmian w oprogramowaniu;
- Opis stosowanej przez COI metodyki testowania oprogramowania.

Przyjęta przez COI metodyka wytwarzania oprogramowania miała charakter iteracyjno-przyrostowy[70].

Testy oprogramowania przeprowadzane przez COI można podzielić na: testy automatyczne (automatyczna realizacja stworzonych przez programistów testów jednostkowych), testy wydajnościowe, testy funkcjonalno-użytkowe przeprowadzane ręcznie (testy zgodności ze specyfikacją wymagań, testy interfejsu użytkownika, testy WCAG[71], jak również testy integracyjne i akceptacyjne), a także testy bezpieczeństwa.

Realizowany przez COI proces zarządzania zmianami, od strony proceduralno-zarządczej był zorganizowany prawidłowo, w sposób typowy dla tego rodzaju procesów.

Zapewnienie bezpieczeństwa systemów ePUAP i PZ

W COI podjęto działania w celu wdrożenia wymagań międzynarodowej normy z zakresu bezpieczeństwa informacji ISO/IEC 27001. Do dnia zakończenia czynności kontrolnych w COI nie w pełni został wdrożony System Zarządzania Bezpieczeństwem Informacji.

W ramach prac wdrożeniowych SZBI podjęto m.in. następujące działania:

- wdrożono *Politykę Bezpieczeństwa Informacji*[72] (dalej: PBI), *Politykę Zarządzania Ciągłością Działania*, *Politykę Ochrony Danych Osobowych*;
- przeprowadzono proces analizy ryzyka, a w 2019 r. przeprowadzono zadanie audytowe o charakterze doradczym przez audytorów wewnętrznych COI pn. *Organizacja i zarządzanie bezpieczeństwem informacji wybranych usług w oparciu o normę ISO/IEC 27001* oraz prze-

[70] Proces zbierania wymagań, projektowania, budowania oraz testowania systemu zorganizowany w krótsze cykle rozwojowe.

[71] Ang. *Web Content Accessibility Guidelines* – wytyczne dla dostępności treści internetowych – to zbiór określający, w jaki sposób uczynić treści internetowe bardziej dostępnymi dla osób niepełnosprawnych.

[72] Na podstawie zarządzenia Dyrektora COI 63/2015 z dnia 26 października 2015 r.

prowadzono weryfikację kompletności i adekwatności procesów oraz dokumentacji bezpieczeństwa informacji, z której sporządzono *Raport z przeglądu SZBI*[73];
- przeprowadzono szkolenie z zakresu przyjętej PBI dla członków zespołu COI-Houston,
- 30 września 2020 r. wydano zarządzenie Nr 93/2020 w sprawie w sprawie powołania w Centralnym Ośrodku Informatyki Systemu Zarządzania Bezpieczeństwem Informacji oraz powołania roli Pełnomocnika ds. SZBI, Audytora ds. SZBI i pozostałych ról wspierających SZBI (dalej: zarządzenie ws. powołania SZBI w COI), które zobowiązało Dyrektora Pionu Operacji COI do wdrożenia do dnia 31 listopada 2020 r. procedur administracyjnych SZBI w zakresie audytowania, monitorowania, oceny, przeglądu oraz doskonalenia SZBI.

W COI w 2015 r. wdrożono PBI, jako komplementarną z politykami systemów ustanowionymi przez MC, obejmującą systemy ePUAP i PZ, w ramach której opracowano szereg procedur szczegółowych[74]. PBI uzupełniono w 2018 r. o Politykę monitoringu[75] oraz w 2020 r. o Politykę zapewniania bezpieczeństwa w zarządzaniu zmianą[76], które zostały wdrożone w COI w wyniku implementacji wymaganych przepisów sankcjonujących proces ochrony danych osobowych, w szczególności przepisów RODO.

W COI sporządzono formalne i udokumentowane polityki i procedury zarządzania tożsamością i kontrolą dostępu do ePUAP/PZ wchodzące w skład PBI (Polityki Bezpieczeństwa Informacji), w tym procedury nadawania, usuwania i modyfikacji uprawnień oraz procedury nadawania praw dostępu fizycznego w COI, a także wnioskowania o dostęp do obiektów współużytkowanych i MC. Uzupełniająco stosowane są instrukcje i podręczniki dla obywateli oraz urzędników opublikowane na stronie www.epuap.gov.pl.

COI nie w pełni wdrożył SZBI, co było niezgodne z § 20 ust. 1, w zw. z ust. 3 rozporządzenia KRI, które stanowią, że podmiot realizujący zadania publiczne opracowuje i ustanawia, wdraża i eksploatuje, monitoruje i przegląda oraz utrzymuje i doskonali system zarządzania bezpieczeństwem informacji zapewniający poufność, dostępność i integralność informacji z uwzględnieniem takich atrybutów, jak autentyczność, rozliczalność, niezaprzeczal-

[73] Raport z dnia 23 grudnia 2019 r., sporządzony przez pracownika COI posiadającego certyfikat Lead Auditor 27001, niebędącego audytorem wewnętrznym COI.

[74] Zgłoszenie i obsługa incydentu bezpieczeństwa PB001, Zabezpieczenia urządzeń przenośnych i ich użytkowanie PB002, Trwałe usuwania danych i niszczenia teleinformatycznych nośników danych PB003, Zarządzanie sprzętem komputerowym PB004, Konfiguracja stacji roboczych urządzeń przenośnych i oprogramowania PB005, Przekazanie nowego systemu do eksploatacji PB006, Zdalne łączenie się w zasobami organizacji Telepraca PB007, Zasady nadawania, usuwania i modyfikacji uprawnień PB008, Metody dostępu do kont uprzywilejowanych PB009, Ochrona antywirusowa PB010, Polityka korzystania z zasobów Internetu PB011, Użytkowanie poczty elektronicznej PB012, Dopuszczenie oprogramowania biurowego do eksploatacji PB013, Zarządzanie nośnikami wymiennymi PB014, Polityka czystego biurka i czystego ekranu PB015.

[75] Wdrożona w COI na podstawie zarządzenia Dyrektora COI z 23 maja 2018 r., które weszło w życie 25 maja 2018 r.

[76] Wdrożona w COI na podstawie zarządzenia Dyrektora COI z 15 czerwca 2020 r.

ność i niezawodność, a wymagania te uznaje się za spełnione, jeżeli system zarządzania bezpieczeństwem informacji został opracowany na podstawie Polskiej Normy PN-ISO/IEC 27001. Zgodnie z § 23 ww. rozporządzenia, systemy teleinformatyczne podmiotów realizujących zadania publiczne funkcjonujące w dniu wejścia w życie rozporządzenia należało dostosować w powyższym zakresie nie później niż w dniu ich pierwszej istotnej modernizacji przypadającej po wejściu w życie tego rozporządzenia. Przepisy te obowiązują od 31 maja 2012 r.

Dyrektor Pionu Operacji COI m.in. wyjaśnił, że SZBI wdrożono w COI *w wyniku wielomiesięcznych prac, zrealizowanych w okresie 2019–2020, związanych z oceną stanu dostosowania istniejących regulacji w COI do wymogów normy ISO/IEC 27001 – I–II kwartał 2019 roku oraz z implementacją wymogów normy ISO/IEC 27001 do funkcjonujących w organizacji procesów biznesowych, operacyjnych i technicznych – II kwartał 2019 – obecnie.* Poinformował, że w COI zaplanowano przeprowadzenie certyfikacji SZBI na zgodność z normą ISO/IEC 27001. W tym celu w I kwartale 2020 r. rozpoczęto postępowanie przetargowe, którego celem było wyłonienie firmy certyfikacyjnej, które w II kwartale 2020 r. *zostało wstrzymane ze względu na ograniczenia wprowadzone z powodu pandemii*. (...) *Postępowanie zostanie wznowione w I kwartale 2021 r., chyba że okoliczności zw. z pandemią COVID-19 (wzrastająca liczba zachorowań) przesuną termin realizacji.* Ponadto wyjaśnił, iż *(...) do 30.11.2020 roku zostaną wdrożone procedury administracyjne SZBI w zakresie auditowania, monitorowania, oceny, przeglądu oraz doskonalenia SZBI. Po zakończeniu pełnego wdrożenia SZBI zostanie przeprowadzony przegląd SZBI w ramach prac Audytora SZBI, na podstawie Procedury audytowania SZBI.*

NIK nie kwestionuje podjęcia przez COI działań w celu wdrożenia SZBI zgodnie z wymaganiami normy ISO/IEC 27001. NIK zauważa jednak, że proces ten trwa w COI już ponad cztery lata i nie został do dnia zakończenia czynności kontrolnych zakończony. W toku kontroli NIK przeprowadzonej w 2016 r. w COI *pt. System Rejestrów Państwowych – bezpieczeństwo, funkcjonowanie i użyteczność* ówczesny Dyrektor COI wyjaśnił, iż trwały wówczas prace przygotowawcze związane z wdrożeniem ww. normy.

Dyrektor COI dopiero 30 września 2020 r. podpisał zarządzenie w sprawie SZBI w COI (wraz ze strukturą zarządczą) oraz zobowiązał Dyrektora Pionu Operacji COI do wdrożenia do dnia 30 listopada 2020 r. procedur administracyjnych SZBI w zakresie audytowania, monitorowania, oceny, przeglądu oraz doskonalenia SZBI. Zatem sam proces wdrożenia będzie ukończony dopiero po wdrożeniu ww. procedur administracyjnych.

W toku kontroli ustalono, iż w COI przeprowadzano półautomatyczne testy bezpieczeństwa[77] m.in. systemów ePUAP i PZ. Z testów tych sporządzano

[77] Polegające na: przygotowaniu listy kontrolnej (tj. listy testów do wykonania), konfiguracja narzędzi, uruchomieniu automatycznych skanerów podatności, manualna weryfikacja wykrytych przez skanery podatności i opracowanie raportu.

raporty, w których posługiwano się pojęciem *testy penetracyjne*[78]. Ustalono, że **COI nie przeprowadził właściwych testów penetracyjnych systemów ePUAP i PZ, co było działaniem nierzetelnym. W ocenie NIK przeprowadzenie pełnych testów jest niezbędne dla uzyskania potwierdzenia, że systemy ePUAP i PZ, które są użytkowane przez obywateli oraz urzędy, są bezpieczne.** Przeprowadzane przez COI testy półautomatyczne bezpieczeństwa nie stanowią testów penetracyjnych w rozumieniu powszechnie przyjętych standardów[79], z uwagi na pominięcie kluczowych faz właściwego ataku, co oznacza, że przeprowadzane przez COI testy nie są testami penetracyjnymi, a jedynie skanowaniem podatności.

Dyrektor Pionu Operacji COI wyjaśnił, *że przyjęta metodyka prowadzenia testów bezpieczeństwa ePUAP/PZ została wypracowana w oparciu o doświadczenia zebrane w trakcie testów bezpieczeństwa prowadzonych w ciągu ostatnich kilku lat. Wspomniana metodyka została dostosowana do procesu wytwórczego oprogramowania, którego istotnym elementem są testy bezpieczeństwa. W przytoczonych przykładach (...) testy bezpieczeństwa obejmowały jedynie zakres wprowadzonych zmian, co było wskazane w poszczególnych raportach z testów. (...) Przed rozpoczęciem testów bezpieczeństwa dokonywana jest weryfikacja ostatecznie wprowadzonych zmian, czy zgodne są z pierwotnymi założeniami i czy przyjęty zakres testów jest prawidłowy. Przyjęta przez Centralny Ośrodek Informatyki metodyka prowadzenia testów bezpieczeństwa w ramach procesu wytwórczego oparta jest o elementy standardu PTES oraz OWASP Testing Guide i zawiera między innymi takie działania jak: Planowanie testów bezpieczeństwa; Określenie i weryfikacja zakresu testów bezpieczeństwa; Zapoznanie się z dokumentacją systemu, wywiad z zespołem wytwórczym; Analiza powierzchni ataku; Przeprowadzenie rekonesansu; Automatyczna identyfikacja znanych podatności; Analiza zidentyfikowanych słabości systemu; Przeprowadzenie działań aktywnych (próba ataku, wykorzystania zidentyfikowanych słabości); Potwierdzenie zidentyfikowanych podatności; Ocena skutków oraz ryzyka dla zidentyfikowanych podatności; Opracowanie rekomendacji odnośnie metod usunięcia podatności, minimalizacji ryzyka; Raportowanie. (...).*

Monitorowanie incydentów bezpieczeństwa jest realizowane w COI przez Security Operation Center (SOC) dla usług świadczonych przez COI na rzecz MC, w tym również na potrzeby monitorowania bezpieczeństwa systemów ePUAP/PZ. Praca SOC odbywa się w trybie ciągłym.

Kopie zapasowe

Polityki tworzenia i testowania kopii zapasowych COI nie zostały opisane w obowiązującej PBI, natomiast zostały zawarte w *Procedurze zarządzania systemem backupowym*, *Procedurze odtworzenia bazy ePUAP* i *Procedurze utrzymaniowej*.

[78] Raport z testów: nForms, system ePUAP2, bezpieczeństwa funkcjonalności „Unieważnienie Profilu Zaufanego", „Przedłużenie Profilu Zaufanego" i „Rejestracja Profilu Zaufanego", bezpieczeństwo komponentu kryptograficznego.

[79] Test penetracyjny, zgodnie z definicją brytyjskiej agencji badawczej NCSC (National Cyber Security Center), jest metodą uzyskiwania pewności co do bezpieczeństwa systemu informatycznego poprzez próbę złamania bezpieczeństwa tego systemu, w całości lub w części, przy użyciu tych samych narzędzi i technik, jakie mógłby zastosować atakujący.

Zdaniem NIK, procedury tworzenia i testowania kopii zapasowych systemów ePUAP oraz PZ wprawdzie zawierają wszystkie wymagane elementy, jednakże dokumenty te mają charakter poradnika administratora, a nie polityk adresowanych do pracowników COI nieznających specjalistycznego systemu do wykonywania kopii zapasowych w sposób zautomatyzowany. **NIK zauważa, że w COI powinna funkcjonować osobna procedura opisująca kompleksowo i zrozumiale politykę tworzenia i przechowywania kopii zapasowych przez COI, a ewentualne szczegółowe rozwiązania dla administratorów wraz z plikami konfiguracyjnymi systemu backupowego mogą stanowić załącznik tego dokumentu.**

W trakcie kontroli NIK, COI dokonał aktualizacji obowiązujących procedur zarządzania systemem backupu ePUAP oraz PZ o elementy związane z przygotowaniem i zatwierdzeniem każdorazowo raportu z przebiegu odtworzenia kopii zapasowych.

Zgodnie z przyjętymi w COI procedurami, kopie zapasowe są tworzone w sposób niezależny w dwóch serwerowniach w trybie przyrostowym (dla serwerów aplikacyjnych) lub pełnym (baza danych systemu ePUAP) za pomocą systemu automatyzującego ten proces i przechowywane są na urządzeniach dyskowych deduplikatora, a także na taśmach magnetycznych. Kopie zapasowe obejmują również tzw. *archive logi*, tj. dziennik zdarzeń obejmujący informacje generowane przez system podczas tworzenia kolejnych kopii zapasowych systemu, co umożliwia podjęcie reakcji na ewentualne błędy pojawiające się w trakcie tego procesu. Kopie bezpieczeństwa przechowywane są w tym samym pomieszczeniu, w którym znajdują się główne serwery aplikacyjne i bazodanowe, co stwarza zagrożenie, że w wypadku katastrofy skutkującej zniszczeniem jednej z serwerowni, zniszczeniu ulegną również kopie zapasowe tam umieszczone. Niezależnie od tego, COI dysponuje zapasowym ośrodkiem danych, posiadającym własne kopie zapasowe, dlatego takie rozwiązanie – zdaniem NIK – należy uznać jako akceptowalne na wypadek wystąpienia awarii.

W toku kontroli ustalono, że kopie zapasowe systemów ePUAP oraz PZ, zgodnie z obowiązującymi procedurami, są regularnie testowane, raz na pół roku.

Plany zapewnienia ciągłości działania systemów ePUAP i PZ w sytuacji wystąpienia znaczącej awarii lub katastrofy

COI przygotował oraz wdrożył rozwiązania techniczne i organizacyjne dla ePUAP i PZ w celu zapewnienia ciągłości działania w sytuacji wystąpienia znaczącej awarii lub katastrofy. Ustanowiono Polityki Zarządzania Ciągłością Działania COI oraz Plan Zarzadzania Kryzysowego i Procedury Ciągłości Działania COI-Houston. Dokumenty te, a w szczególności Polityka Zarządzania Ciągłością Działania COI, regulują m.in. zagadnienia dotyczące:

- określenia struktury i planu zarządzania kryzysowego, w tym składu i trybu działania, komunikacji Sztabu Kryzysowego COI, jak również określenia poziomów gotowości alarmowej i zasad wzmożonego monitorowania;

- konieczności utrzymywania Procedur Ciągłości Działania oraz Procedur Odtworzenia dla poszczególnych komórek organizacyjnych COI oraz zasady ich dystrybucji i aktualizacji;
- zasady wykonywania testów Procedur Ciągłości Działania;
- zasady raportowania zagrożeń;
- konieczności wykonywania analizy BIA[80].

W COI wdrożono rozwiązania w zakresie odtworzenia infrastruktury po katastrofie poprzez zastosowanie podwójnej redundancji (nadmiarowości), polegającej na utrzymywaniu dwóch równoległych ośrodków przetwarzania danych oraz zabezpieczono zasoby ludzkie do utrzymania tych systemów w przypadku absencji pracowników przez redundancję osobową. Oba ośrodki zawierają te same bazy danych systemów ePUAP i PZ oraz ten sam zestaw serwerów aplikacyjnych. W obrębie każdego z dwóch ośrodków wykonywane są kopie zapasowe. W razie awarii, bądź zniszczenia ośrodka głównego, jego zadania przejmuje ośrodek zapasowy.

W COI stosowana jest praktyka w zakresie zapewniania środków redundancji, tj. procedura przełączania systemów ePUAP i PZ z ośrodka głównego na zapasowy oraz testów procedury odtwarzania baz danych z kopii zapasowych. W toku kontroli ustalono, iż wykonywane są testy odtwarzania baz danych dwa razy do roku oraz prowadzone są testy przełączania systemów ePUAP i PZ z ośrodka głównego na zapasowy jeden raz do roku. Z testów tych sporządzane są raporty. Z analizy tych dokumentów wynika, iż wszystkie testy przełączeniowe przebiegły pozytywnie, a czas przełączania systemu ePUAP z ośrodka głównego na zapasowy wynosił: 25 minut w kwietniu 2019 r., 37 minut w marcu 2020 r. oraz 2 godziny i 32 minuty w kwietniu 2020 r. Dyrektor Pionu Operacji COI wyjaśnił, iż przełączenie tylko bazy danych jest szybsze niż przełączenie wszystkich serwerów aplikacyjnych, a testy przełączania obejmowały wyłączenie serwerów aplikacyjnych, co jest czasochłonne i robi się to dla bezpieczeństwa bazy danych.

Zdaniem NIK, przyjęte przez COI rozwiązania techniczne i organizacyjne są właściwe dla zapewnienia ciągłości działania systemów ePUAP i PZ w sytuacji wystąpienia znaczącej awarii lub katastrofy.

Audyty bezpieczeństwa systemu ePUAP

W COI na zlecenie MC przeprowadzono audyt bezpieczeństwa systemu ePUAP przez zewnętrzny podmiot specjalizujący się w wykonywaniu tego rodzaju audytów. Dyrektor Pionu Operacji COI wyjaśnił, że *wszystkie możliwe do realizacji zalecenia z raportu zostały bezzwłocznie zrealizowane, natomiast z uwagi na fakt, iż raport ten nie był przed sporządzeniem konsultowany z COI, część z zaleceń było niemożliwych do wykonania lub generowały ryzyko w obszarach nieznanych audytorom* (...).

[80] BIA – ang. *Business Impact Analysis* – analiza wpływu na działalność, jest to proces analizy funkcji biznesowych pozwalający określić, jaki wpływ na działalność organizacji miałoby ich ewentualne poważne zakłócenie lub przerwanie.

5.3. Świadczenie przez urzędy jednostek samorządu terytorialnego usług drogą elektroniczną poprzez ePUAP

JST zapewniły sprawne świadczenie e-usług. Wdrożono rozwiązania w zakresie zapewnienia ich bezpieczeństwa jednak w wielu urzędach wystąpiły nieprawidłowości.

Kontrolą objęto 28 urzędów miast oraz gmin. Kwestie dostosowania urzędów do świadczenia usług w formie elektronicznej były uwzględnione w dokumentach strategicznych w przypadku 68% badanych urzędów. W niemal wszystkich kontrolowanych urzędach (w 27 z 28, tj. w 96%) podstawowym sposobem dokumentowania przebiegu i rozstrzygania spraw był jednak system tradycyjny (papierowy), wspomagany przez systemy elektronicznego obiegu dokumentów. W ośmiu urzędach (tj. w 29%) za pośrednictwem platformy ePUAP obywatele mogli skorzystać z ponad 50 e-usług. Na podstawie analizy próby 567 spraw zrealizowanych w formie e-usług stwierdzono, że były one załatwiane bez zbędnej zwłoki, z wykorzystaniem informacji znajdujących się w urzędzie oraz danych zgromadzonych w innych rejestrach publicznych, bez zobowiązywania wnioskodawców do dostarczania dodatkowych informacji lub dokumentów będących w posiadaniu urzędu lub innych urzędów administracji publicznej.

W badanych urzędach, poza jednym wyjątkiem, podejmowano działania w celu informowania obywateli o możliwości załatwienia spraw drogą elektroniczną w formie e-usług. Jednak aż w 33% urzędów udostępniane informacje o świadczonych e-usługach na stronach internetowych były niekompletne, mało czytelne i trudne do odnalezienia.

Kontrolowane urzędy w większości przypadków nie zapewniły należytej organizacji bezpieczeństwa informacji. W 57% urzędów brak było Systemu Zapewnienia Bezpieczeństwa Informacji, a w 39% urzędów brakowało też pełnej i aktualnej informacji o posiadanych zasobach informatycznych służących do przetwarzania danych. W 21% urzędów część użytkowników systemów informatycznych posiadała uprawnienia administracyjne, pomimo, iż nie byli pracownikami służb informatycznych, w związku z czym użytkownicy mogli samodzielnie instalować dowolne oprogramowanie. Ponadto, kontrolowane urzędy nie podejmowały wystarczających działań w zakresie oceny wdrożonych rozwiązań bezpieczeństwa informacji, gdyż w 54 % z nich nie przeprowadzano obowiązkowych audytów w zakresie bezpieczeństwa informacji. Również wcześniejsze kontrole NIK[81], w których badano wybrane aspekty bezpieczeństwa informacji, wykazały wiele nieprawidłowości w tym zakresie. Pozytywnie natomiast należy ocenić, że w 82% urzędów zorganizowano szkolenia w zakresie bezpieczeństwa informacji.

Działania strategiczne w celu umożliwienia załatwiania spraw drogą elektroniczną w urzędach miast oraz gmin

W dokumentach strategicznych większości kontrolowanych urzędów[82] (19 spośród 28, tj. 68%) uwzględniono zagadnienia dotyczące ich dostoso-

[81] M.in.: P/17/062/LBI *Bezpieczeństwo elektronicznych zasobów informacyjnych w jednostkach samorządu terytorialnego w Województwie Podlaskim* (nr. ewid. 100/2018/P/17/062/LBI, październik 2018 r.); P/18/006 *Zarządzanie bezpieczeństwem informacji w jednostkach samorządu terytorialnego* (nr ewid. 187/2018/P/18/006/KAP, luty 2019 r.).

[82] UM w: Aleksandrowie Łódzkim, Augustowie, Białogardzie, Gryfinie, Legionowie, Łomży, Myszkowie, Obornikach, Oleśnicy, Oławie, Piastowie, Policach, Sochaczewie, Śremie, Swarzędzu, Wałczu, Wolsztynie, Ząbkach, Zgorzelcu.

wania do elektronicznego świadczenia usług publicznych. W dokumentach tych przyjęto cele i określono działania dotyczące rozwoju społeczeństwa cyfrowego i zwiększenia dostępu do e-usług, w tym uwzględniano problematykę związaną m.in. z takimi zadaniami jak:

- rozszerzenie zakresu e-usług publicznych;
- usprawnienie administracji publicznej poprzez informatyzację, m.in. zwiększenie dostępności usług publicznych przy wykorzystaniu Internetu;
- zapewnienie mieszkańcom dostępu do usług publicznych świadczonych drogą elektroniczną.

Przykład

W ***Strategii Rozwoju Gminy Miejskiej Legionowo do roku 2030***[83] wskazano cel strategiczny *Wzmocnienie integracji społecznej,* w ramach którego wyznaczono cel operacyjny *Zwiększenie wykorzystania e-usług publicznych w Legionowie*. W opisie celu wskazano, m.in. że *Udostępnienie możliwości załatwiania jak najszerszego zakresu czynności i spraw urzędowych poprzez wykorzystanie nowoczesnych możliwości jakie daje Internet będzie stanowić duże ułatwienie dla mieszkańców i sprawi, że urząd i inne instytucje publiczne okażą się o wiele sprawniejsze, jak i przyjaźniejsze umożliwiając maksymalnie wygodny i jednoznaczny kontakt.* Ponadto, Strategia w rozdziale *Kierunki działań w realizacji strategii* wskazuje, że wzmocnienie integracji społecznej będzie realizowane poprzez zwiększanie wykorzystania e-usług w kilku obszarach (e-administracja, e-kultura, e-zdrowie, e-turystyka, e-transport, rozwój społeczeństwa cyfrowego). Stopień realizacji celów Strategii był monitorowany zgodnie z jej postanowieniami, co zostało potwierdzone w *Raporcie z monitoringu Strategii Rozwoju Gminy Miejskiej Legionowo do roku 2030 za lata 2017–2018.*

Liczba udostępnionych i zrealizowanych usług elektronicznych w kontrolowanych urzędach

Według stanu na dzień 31 maja 2020 r. kontrolowane urzędy[84] na platformie ePUAP udostępniały łącznie 1 402 usługi elektroniczne, w tym usługę ESP (Elektroniczna Skrzynka Podawcza), która polega na możliwości skierowania do urzędu pisma ogólnego, skargi, wniosku czy też zapytania oraz załączenia odpowiedniego formularza w wersji elektronicznej zapisanego w określonym formacie (np. .pdf, .doc).

Najwięcej usług w formie elektronicznej zostało udostępnionych w takich dziedzinach jak: sprawy obywatelskie (dowody osobiste, meldunki, wybory); budownictwo, architektura, urbanistyka; podatki i opłaty oraz nieruchomości, lokale mieszkalne i użytkowe; ochrona środowiska.

Więcej niż 50 usług w formie elektronicznej udostępniano poprzez ePUAP w ośmiu[85] spośród 28 skontrolowanych urzędów (tj. 29%). W pozostałych badanych urzędach oferowano od 10 do 50 e-usług[86].

---

[83] Wprowadzona Uchwałą Nr XXVIII/357/2017 Rady Miasta Legionowo z dnia 28 lutego 2017 r. w sprawie przyjęcia *Strategii Rozwoju Gminy Miejskiej Legionowo do roku 2030*.

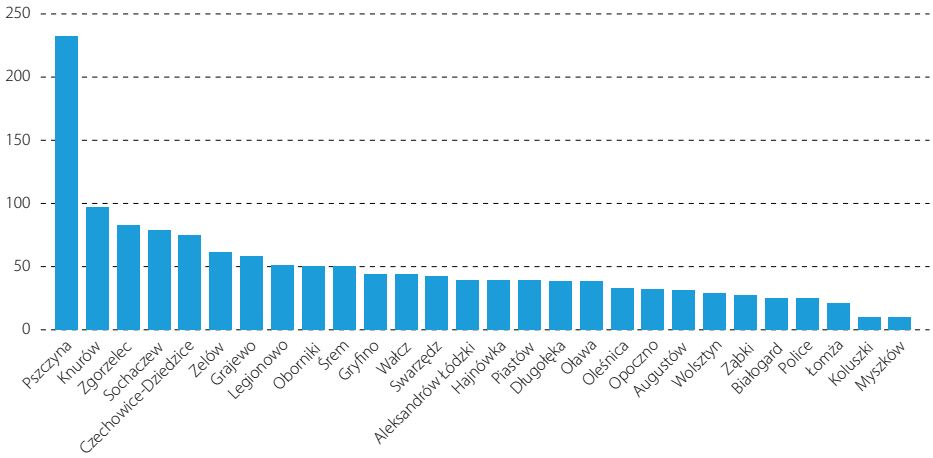
[84] UM w Łomży – stan na 30 czerwca 2020 r., UM w: Legionowie i Zgorzelcu – stan na 15 lipca 2020 r., UM w Oleśnicy – stan na 11 sierpnia 2020 r.

[85] UM w (liczba udostępnionych e-usług): Czechowicach-Dziedzicach (75), Grajewie (58), Knurowie (97), Legionowie (51), Pszczynie (232), Sochaczewie (79), Zelowie (61) i Zgorzelcu (83).

[86] UM w (w nawiasie liczba udostępnionych e-usług): Aleksandrowie Łódzkim (39), Augustowie (31), Białogardzie (25), Gryfinie (44), Hajnówce (39), Koluszkach (10), Łomży (21), Myszkowie (10), Obornikach (50), Oleśnicy (33), Oławie (38), Opocznie (32), Piastowie (39), Policach (25), Śremie (50), Swarzędzu (42), Wałczu (44), Wolsztynie (29), Ząbkach (27), a także w UG w Długołęce (38).

Infografika nr 7

Liczba udostępnionych e-usług na ePUAP na dzień 31 maja 2020 r.



Źródło: opracowanie własne NIK na podstawie danych z kontroli.

W kontrolowanych urzędach liczba e-usług zrealizowanych przez obywateli w okresie od 1 stycznia 2020 r. do 30 czerwca 2020 r. wyniosła łącznie 30 580 e-usług. Najczęściej korzystali oni z e-usług w zakresie: złożenia pisma ogólnego, spraw obywatelskich (akty stanu cywilnego, dowody osobiste, meldunki, wybory), wniesienia skargi oraz zapytania do urzędu (ESP).

We wszystkich kontrolowanych urzędach w okresie od 1 marca do 30 czerwca 2020 r., tj. w okresie epidemii COVID-19 w Polsce nastąpił duży wzrost zainteresowania e-usługami.

Przykłady

W **Urzędzie Miasta i Gminy w Gryfinie** w okresie od 1 stycznia 2020 r. do 30 czerwca 2020 r. w Urzędzie zrealizowano łącznie 506 e-usług, w tym od 1 stycznia 2020 r. do 29 lutego 2020 r. – 108, od 1 marca 2020 r. do 30 kwietnia 2020 r. – 107 oraz od 1 maja 2020 r. do 30 czerwca 2020 r. – 291. Najwięcej e-usług zrealizowano w zakresie: dopisania się do spisu wyborców (152), uzyskania dowodu osobistego (116), pism ogólnych, skarg, wniosków, zapytań do urzędu (97), zgłoszenia zameldowania/wymeldowania (58), wydania odpisu aktu stanu cywilnego (40), dopisania się do rejestru wyborców (10), zgłoszenia utraty dowodu osobistego (10), deklaracji na podatek od nieruchomości (5). W I półroczu 2020 r. 29 e-usług (z 44 dostępnych ogółem w Urzędzie) zrealizowano w liczbie poniżej pięciu każda[87].

W **Urzędzie Miejskim w Aleksandrowie Łódzkim** w pierwszym półroczu 2020 r. za pośrednictwem e-PUAP w Urzędzie zrealizowano 1642 usługi elektroniczne, z czego: 223 usługi w okresie od 1 stycznia 2020 r. do 28 lutego 2020 r., 584 usługi w okresie od 1 marca 2020 r. do 30 kwietnia 2020 r., 835 usług w okresie od 1 maja 2020 r. do 30 czerwca 2020 r. Najwięcej spraw dotyczyło: dopisania do spisu wyborców (430 wniosków lub zawia-

[87] Tj. np. deklaracja o wysokości opłaty za gospodarowanie nieruchomościami; deklaracja na podatek rolny; deklaracja na podatek leśny; deklaracja na podatek od środków transportowych; informacja w sprawie podatku od nieruchomości; informacja w sprawie podatku rolnego; zgłoszenie urodzenia dziecka; wydanie wypisu i wyrysu ze studium uwarunkowań i kierunków zagospodarowania przestrzennego.

domień, tj. 26,2% wszystkich e-usług w tym okresie), spraw meldunkowych (253, tj. 15,4%) oraz wydania dowodu osobistego (237, tj. 14,4%). Pozostałe wnioski i zawiadomienia głównie dotyczyły: geodezji88 (181, tj. 11%), pomocy społecznej (85, tj. 5,2%), gospodarki komunalnej (84, tj. 5,1%) oraz podatków (55, tj. 3,3%). W okresie od 1 marca 2020 r. do 30 kwietnia 2020 r. znacznie częściej występowano do Urzędu: w sprawach meldunkowych (wzrost o 768%), dotyczących rolnictwa (wzrost o 300%) oraz w sprawach dotyczących aktów stanu cywilnego (wzrost o 229%) i pomocy społecznej (wzrost o 207%). W trakcie kolejnych dwóch miesięcy (maj–czerwiec 2020 r.) liczba spraw kierowanych do Urzędu przez ePUAP była o 274% wyższa od złożonych na początku roku (styczeń–luty 2020 r.) i o 43% wyższa niż w miesiącach marzec–kwiecień 2020 r.

Procedury obiegu (zarządzania) dokumentami, regulujące komunikację elektroniczną i załatwianie spraw w urzędzie w formie elektronicznej

W 27 z 28 (96%) kontrolowanych urzędów jako podstawowy sposób dokumentowania przebiegu załatwiania i rozstrzygania spraw, wskazywano system tradycyjny (papierowy) wykonywania czynności kancelaryjnych w urzędzie wspomagany przez elektroniczne systemy obiegu dokumentów (EZD) na różnych etapach załatwiania spraw w urzędzie.

Przykład

W **Urzędzie Miejskim w Łomży** podstawowym sposobem wykonywania czynności kancelaryjnych (dokumentowania przebiegu realizacji i rozstrzygania spraw) był system tradycyjny, tj. papierowy. W związku z realizacją projektu pn. „Wdrożenie elektronicznych usług dla ludności województwa podlaskiego – część II administracja samorządowa”[89], zakładającego wdrożenie do użytkowania programu elektronicznego zarządzania dokumentacją („EZD SmartDoc”) w Urzędzie od 2016 roku wprowadzono teleinformatyczny system do elektronicznego zarządzania dokumentacją, jako system wspomagający. Tradycyjny systemem prowadzenia dokumentacji pozostał obowiązującym, jednak sprawy, które wpływały do Urzędu na nośniku papierowym były rejestrowane przez sekretariat Urzędu w systemie EZD (w tym skanowane w celu wprowadzenia do obrotu elektronicznego w tym systemie). W przypadku spraw wpływających za pośrednictwem platformy ePUAP sposób ich realizacji uzależniony był od życzenia wnioskodawcy. I tak:

- jeżeli wnioskodawca wskazał, że chce, aby jego sprawa została zrealizowana w sposób tradycyjny (papierowy) – wówczas wszystkie pisma były sporządzane w sposób tradycyjny i wysyłane wnioskodawcy za pośrednictwem poczty, a dokumentacja przechowywana była w formie papierowej w teczkach spraw;
- jeżeli wnioskodawca wskazał, że chce, aby jego sprawa wykonana została elektronicznie – wówczas wszystkie pisma były przesyłane wnioskodawcy za pośrednictwem platformy ePUAP, a dokumenty w sprawie przechowywane były w formie papierowej (podstawowy system dokumentowania przebiegu załatwiania i rozstrzygania spraw) i w elektronicznej (w elektronicznym systemie zarządzania dokumentami).

[88] Dotyczy m.in. stanu prawnego nieruchomości, wniosków o wypis i wyrys z miejscowego planu zagospodarowania przestrzennego, ewidencji gruntów, nabycia gruntu, przeznaczenia gruntu, numeru porządkowego nieruchomości.

[89] Projekt realizowany w ramach Regionalnego Programu Operacyjnego Województwa Podlaskiego na lata 2007–2013 Osi Priorytetowej IV *Społeczeństwo informacyjne* nr WND-RPPD.04.01.00-20-002/11.

W jednym urzędzie[90] jako podstawowy sposób dokumentowania przebiegu załatwiania i rozstrzygania spraw, wskazany został system elektronicznego zarządzania dokumentacją.

W czterech urzędach[91] nie opracowano procedur obiegu dokumentów regulujących komunikację elektroniczną oraz załatwiania spraw w formie elektronicznej pomimo, że w urzędach tych w rzeczywistości dominującą formą załatwiania i rozstrzygania spraw był obieg elektroniczny.

Przykład

W **Urzędzie Miasta Zgorzelec** pomimo powszechnego stosowania EOD jako sposobu pomocniczego w zakresie dokumentowania przebiegu załatwiania i rozstrzygania spraw, nie opracowano procedur EOD oraz załatwiania spraw w formie elektronicznej, w tym weryfikacji podpisów elektronicznych. W ocenie NIK, zaniechanie to świadczy o nierzetelności, gdyż funkcjonujące wewnętrzne uregulowania nie uwzględniały stanu rzeczywistego, tj. pomimo przyjęcia tradycyjnego (papierowego) sposobu dokumentowania, znacząca liczba spraw była dokumentowana elektronicznie. Zastępca Burmistrza wyjaśnił, że formalnie nie uregulowano procedur w tym zakresie, ale w najbliższym czasie zostanie to wykonane.

Realizowanie usług elektronicznych wpływających do urzędów j.s.t. poprzez ePUAP

Badanie prawidłowości realizacji e-usług przeprowadzono w 28 skontrolowanych urzędach na łącznej próbie 567 spraw, które wpłynęły drogą elektroniczną za pośrednictwem ePUAP. Dotyczyło takich rodzajów e-usług jak: sprawy obywatelskie (dowody osobiste, meldunki, akty stanu cywilnego, wybory); pismo ogólne, skargi, wnioski, zapytania do urzędu; geodezja; gospodarka komunalna; podatki i opłaty.

Szczegółowa analiza próby 567 spraw wykazała, że:

- dekretacja dokumentów elektronicznych (od momentu wpływu/rejestracji wniosku/formularza) następowała na ogół niezwłocznie. Wystąpiły także pojedyncze przypadki, kiedy dekretacji sprawy do załatwienia dokonano po upływie kilkunastu dni co tłumaczono przeoczeniem;
- w 21 urzędach[92] część analizowanych wniosków/formularzy wymagała korekt i uzupełnień z powodu błędów w wypełnianiu przez wnioskodawców. W żadnym z kontrolowanych urzędów nie wymagano osobistego stawiennictwa obywatela w celu uzupełnienia wniosku. Informacje o konieczności dokonania korekty przekazywano przy wykorzystaniu ePUAP, poczty elektronicznej, telefonicznie lub pocztą tradycyjną;
- we wszystkich kontrolowanych urzędach możliwe było uzyskanie informacji na temat aktualnego stanu załatwianej sprawy. Informacje takie można było uzyskać elektronicznie, np. mailem, przez stronę BIP lub poprzez ePUAP, a także drogą telefoniczną;

[90] UM w Oleśnicy.

[91] UM w: Oławie, Wolsztynie i Zgorzelcu, a także UG w Długołęce.

[92] UM w: Aleksandrowie Łódzkim, Gryfinie, Hajnówce, Knurowie, Koluszkach, Legionowie, Łomży, Myszkowie, Oleśnicy, Oławie, Opocznie, Piastowie, Policach, Pszczynie, Sochaczewie, Śremie, Wałczu, Ząbkach, Zelowie i Zgorzelcu, a także UG w Długołęce.

– przy załatwianiu spraw pracownicy wszystkich kontrolowanych urzędów korzystali z danych gromadzonych w zewnętrznych systemach i rejestrach państwowych takich jak np. PESEL, Rejestr Dowodów Osobistych, Elektroniczne Księgi Wieczyste, Baza Usług Aktów Stanu Cywilnego, Ewidencja Gruntów i Budynków.

Monitoring poziomu wykorzystania e-usług realizowanych poprzez ePUAP

W 10 z 28 kontrolowanych urzędów[93] poziom wykorzystania e-usług realizowanych przez ePUAP był objęty bieżącym monitoringiem.

Przykłady

W **Urzędzie Miasta Białogard** codziennie z systemu obiegu dokumentów eDOK (powiązanego z ePUAP) drukowany był raport poczty przychodzącej z uwzględnieniem korespondencji wpływającej do Urzędu za pośrednictwem ePUAP. System eDOK umożliwiał generowanie raportów cząstkowych za wskazany okres (np. według dekretacji do poszczególnych wydziałów Urzędu, raporty poczty przychodzącej i wychodzącej), które służyły do analiz wykorzystania usług ePUAP.

W **Urzędzie Miasta i Gminy w Swarzędzu** bieżący monitoring realizowany był poprzez integrację platformy ePUAP z systemem EZD, służącym do zarządzania i elektronicznego obiegu dokumentów w Urzędzie. Liczba świadczonych usług i spraw załatwianych drogą elektroniczną była na bieżąco monitorowana przez pracowników Wydziału Teleinformatyki. Wyniki monitoringu załatwianych spraw i świadczonych e-Usług w okresie objętym kontrolą poddawane były analizie, a na jej podstawie pracownicy Wydziału Teleinformatyki i Wydziału Promocji podejmowali działania mające na celu rozpowszechnienie informacji o e-usługach świadczonych w ramach eUrzędu i platformy ePUAP.

Skargi dotyczące świadczenia usług publicznych w formie elektronicznej

W 26 urzędach nie odnotowano wpływu skarg w zakresie świadczenia usług publicznych w formie elektronicznej, ani wniosków w sprawie usprawnienia tej formy komunikacji. W pozostałych dwóch kontrolowanych urzędach[94] wpłynęły łącznie trzy skargi w tym zakresie. Skargi dotyczyły m.in.:

– braku informacji o adresie do korespondencji przy użyciu ePUAP do systemu obsługi naliczeń wynagrodzeń dla pracowników i innych świadczeniobiorców. W następstwie skargi wprowadzono właściwy adres w systemie i doręczono korespondencję w sposób wskazany przez wnioskodawcę. Zapewniono, że dalsza korespondencja będzie kierowana do wnioskodawcy przy wykorzystaniu ePUAP;
– informacji przekazanej wnioskodawcy o braku możliwości oceny zasadności złożonej skargi dotyczącej deklaracji o wysokości opłaty za gospodarowanie odpadami komunalnymi ze względu na jej ogólnikowość i brak podstawowych danych dotyczących obsługiwanej osoby oraz adresu nieruchomości.

Działania w zakresie zapewnienia stałego i nieprzerwanego działania EZD

W 27 (96%) jednostkach w celu zapewnienia sprawnego i nieprzerwanego działania systemu elektronicznego obiegu dokumentów, zawarto stosowne umowy serwisowe, które obowiązywały w całym okresie objętym kontrolą. W powyższych umowach zdefiniowane zostały m.in. awarie krytyczne

[93] UM w: Białogardzie, Czechowicach-Dziedzicach, Knurowie, Koluszkach, Legionowie, Łomży, Opocznie, Śremie, Swarzędzu, Zelowie.

[94] UM w: Legionowie (dwie skargi) i Oławie (jedna skarga).

i niekrytyczne oraz usterki, a także ustalone zostały zasady postępowania w przypadku ich wystąpienia. Określony został również „czas reakcji" wykonawcy na zgłoszenie wadliwego działania systemu oraz czasy usunięcia awarii w zależności od jej istotności.

Jedynie w jednym spośród 28 (4%) kontrolowanych urzędów wystąpiły nieprawidłowości w zakresie zapewnienia sprawnego i nieprzerwanego działania elektronicznego obiegu dokumentów.

Przykład

W **Urzędzie Miejskim w Zelowie** przy zawieraniu umów z producentem systemu EZD, obowiązujących w latach 2016–2020, nie określono kategorii zgłoszeń (np. błąd krytyczny, poważny, drobny) oraz czasu na usunięcie ewentualnych usterek oprogramowania, przez co nie zagwarantowano maksymalnego czasu, po jakim ma być przywrócone prawidłowe funkcjonowanie systemu.

Zgłoszenia problemów technicznych przez urzędy, dotyczących funkcjonowania platformy ePUAP

Większość kontrolowanych urzędów[95] (20 z 28, tj. 71%) zgłaszało w okresie od 1 stycznia 2020 do 30 czerwca 2020 r. awarie w funkcjonowaniu ePUAP. Zgłoszenia dotyczyły m.in.: braku dostępności do platformy z powodu prowadzonych prac serwisowych; rozmiaru dokumentu elektronicznego wraz z załącznikami, który można wysłać przez ePUAP; formularza o wydanie zaświadczenia o figurowaniu/niefigurowaniu w ewidencji podatników podatków i opłat; opóźnień wpływu pism na skrzynkę podawczą; niedziałającego podglądu podczas edycji formularza; braku możliwości zaadresowania deklaracji na podatek od środków transportowych; braku potwierdzenia elektronicznego wniesienia opłaty za wniosek o odpis aktu stanu cywilnego złożonego przez ePUAP.

Przykład

W **Urzędzie Miasta Oleśnicy** problemy z funkcjonowaniem platformy ePUAP zdarzały się wielokrotnie, a ich nasilenie nastąpiło w okresie od marca do lipca 2020 r., kiedy wzrosła znacznie liczba składanych wniosków. Głównymi objawami awarii były m.in. wielokrotne automatyczne „wylogowywanie" osoby użytkującej system oraz brak możliwości wczytywania plików i zawieszanie się strony internetowej. W przypadku wystąpienia ww. problemów informatycy Urzędu zgłaszali je do COI, na skrzynkę pocztową *pomoc@coi.gov.pl* lub poprzez dedykowaną do tego celu aplikację *Atmosfera.* Czas oczekiwania na pierwszą odpowiedź od COI był zróżnicowany i wynosił od dwóch tygodni do czterech miesięcy. Zdaniem Informatyka Urzędu niektóre z odpowiedzi COI na zgłoszone awarie i problemy nie były adekwatne do zgłoszenia, a zaproponowane rozwiązania nie skutkowały przywróceniem możliwości użytkowania platformy ePUAP[96]. Urząd nie zidentyfikował sytuacji, w której problemy z funkcjonowaniem ESP na ePUAP miały wpływ na terminowość załatwiania spraw.

[95] UM w: Aleksandrowie Łódzkim, Czechowicach-Dziedzicach, Grajewie, Gryfinie, Hajnówce, Koluszkach, Legionowie, Łomży, Myszkowie, Obornikach, Oleśnicy, Oławie, Opocznie, Piastowie, Sochaczewie, Wałczu, Wolsztynie, Ząbkach, Zelowie i Zgorzelcu.

[96] COI wskazywał np. na usunięcie historii przeglądania stron internetowych przeglądarki internetowej czy ponowne uruchomienie przeglądarki, co w opinii Informatyka jest pierwszą czynnością wykonywaną przy tego typu sytuacjach bez zawiadamiania COI.

Działania informacyjno-promocyjne dotyczące możliwości załatwienia spraw drogą elektroniczną

Spośród 28 kontrolowanych urzędów tylko w jednym urzędzie[97] nie podejmowano żadnych działań w celu informowania obywateli o możliwości załatwienia spraw drogą elektroniczną co NIK oceniła jako nierzetelne.

Przykład

Na stronie internetowej **Urzędu Gminy Długołęka** nie zamieszczono informacji na temat Elektronicznej Skrzynki Podawczej ePUAP, nie zawarto listy spraw możliwych do załatwienia w formie e-usług oraz informacji, że w celu skorzystania z e-usług przez obywatela, konieczne jest posiadanie profilu zaufanego lub „nowego" dowodu osobistego z warstwą elektroniczną. Nie zawarto też czytelnej informacji o sposobie uzyskania profilu zaufanego oraz żadnej informacji dotyczącej „nowego" dowodu osobistego z warstwą elektroniczną. Wójt Gminy wyjaśnił, że stwierdzony w trakcie oględzin brak usystematyzowanej informacji na temat e-usług zostanie w najbliższym czasie uzupełniony.

Wśród 27 urzędów, które na swoich stronach internetowych i BIP zamieszczały informacje o możliwości załatwienia spraw drogą elektroniczną, w dziewięciu[98] (33%) informacje w tym zakresie były niekompletne, mało czytelne i trudne do odnalezienia na stronach internetowych urzędów.

Przykłady

Zamieszczone na stronie internetowej **Urzędu Miejskiego w Zelowie** informacje o możliwości załatwienia spraw drogą elektroniczną były niekompletne i trudne do odnalezienia. Pomimo, iż na stronie internetowej Urzędu przewidziano sposób komunikowania zainteresowanym o sposobie i warunkach realizacji e-usług poprzez ePUAP, informacje tam zawarte nie wskazywały spraw możliwych do procedowania drogą elektroniczną. Wyszukanie tych danych wymagało przeanalizowania zakresu świadczonych usług na stronie BIP Urzędu, które nie były kompletne i aktualne. Ponadto, na stronie internetowej urzędu nie zawarto informacji o możliwości posługiwania się nowym dowodem z warstwą elektroniczną przy kontaktach z Urzędem drogą elektroniczną.

Urząd Miasta Piastowa nie zapewnił należytego informowania obywateli o funkcjonalnościach nowego e-dowodu osobistego. Na stronie Urzędu www.piastow.pl nie wskazano, że nowy dowód osobisty może – na wniosek zainteresowanego – zawierać podpis elektroniczny, pozwalający na korzystanie z usług elektronicznych. IOD (*Inspektor Ochrony Danych)* wyjaśnił.: *...w chwili wydawania obywatelom ‚nowych' dowodów osobistych z warstwą elektroniczną pracownicy urzędu każdorazowo informują mieszkańców o sprawach możliwych do załatwienia przy użyciu tego dowodu*.

Zdaniem NIK, brak skutecznych działań informacyjnych na temat możliwości załatwiania spraw drogą elektroniczną, może być jedną z przyczyn ograniczonego zainteresowania możliwością korzystania z usług publicznych w formie elektronicznej.

NIK zwraca uwagę na potrzebę podjęcia przez organy jednostek samorządu terytorialnego szerszych działań w zakresie informowania o e-usługach, co mogłoby wpłynąć na większe zainteresowanie mieszkańców możliwością załatwiania spraw w urzędzie drogą elektroniczną.

[97] UG Długołęka.

[98] UM w: Augustowie, Hajnówce, Koluszkach, Obornikach, Oleśnicy, Oławie, Piastowie, Wolsztynie i Zelowie.

NIK wskazuje, że funkcjonalności nowego dowodu mogą być zastosowane przy elektronicznym załatwianiu spraw, dlatego też ważne jest umieszczenie informacji o nich na stronach internetowych urzędów w miejscu, w którym te sprawy są opisane z informacją, że mogą być załatwiane w postaci e-usługi.

W pozostałych 18 urzędach[99] (z 27, tj. w 67%) nie stwierdzono nieprawidłowości w badanym zakresie. Na stronach internetowych urzędów lub BIP zamieszczano m.in. listy spraw możliwych do załatwienia w formie e-usług, a w przypadku gdzie konieczne było posiadanie profilu zaufanego lub „nowego" dowodu osobistego z warstwą elektroniczną, wskazywano na taką konieczność, podawano informacje dotyczące metod i wymagań dostarczania dokumentów elektronicznych, np. o potrzebie załączenia do wniosku załączników oraz wniesienia opłat, znajdowały się też informacje o terminie załatwienia danej sprawy.

Przykład

Na stronie internetowej **Urzędu Miasta Wałcz** zamieszczono informacje o możliwości załatwienia spraw drogą elektroniczną[100]. Na tej stronie w trzech zakładkach w jasnej i czytelnej formie podano informacje: dotyczące dostarczania dokumentów (metody dostarczania dokumentów); wymagania dla dokumentów elektronicznych dostarczanych do Urzędu; zamieszczono uwagę, że aby można było złożyć wniosek do urzędu drogą elektroniczną konieczne jest posiadanie konta użytkownika na platformie ePUAP. Zakładka „skrzynka ePUAP" zawierała praktyczne informacje o sposobie korzystania z platformy e-PUAP oraz o sposobie dostarczenia i podpisania pisma. Zakładka „Profil zaufany" zawierała informacje, w jaki sposób założyć profil zaufany wraz z metodą autoryzacji oraz rejestracji konta w Profilu Zaufanym. Informacja o sposobie uzyskania „nowego" dowodu osobistego z warstwą elektroniczną podana została przy opisie usługi Dowody osobiste: składanie wniosku o wydanie dowodu osobistego w formie dokumentu elektronicznego na stronie BIP Urzędu. Opisano m.in. od kiedy weszły przepisy, na podstawie których wydawane są dowody osobiste z warstwą elektroniczną, kto może złożyć wniosek o e-dowód oraz sposób jego odbioru. Podano również wymagania dotyczące fotografii oraz odnośnik do wniosku o wydanie dowodu osobistego w formie dokumentu elektronicznego. W opisie procedury podano informacje o funkcjach warstwy elektronicznej dowodu.

Szkolenia dotyczące e-usług oraz bezpieczeństwa danych

Stosownie do § 20 ust. 2 pkt 6 rozporządzenia KRI, w 23 urzędach[101] (82%) zorganizowano szkolenia dla pracowników zaangażowanych w proces przetwarzania informacji z zakresu komunikacji elektronicznej oraz zagrożeń z tym związanych (w tym dotyczących bezpieczeństwa informacji). Tematyka szkoleń obejmowała m.in.: zagrożenia związane z obsługą systemów informatycznych i programów komputerowych, cyberbezpieczeństwo i bezpieczeństwo infrastruktury IT, ochronę informacji RODO

[99] UM w: Aleksandrowie Łódzkim, Białogardzie, Czechowicach-Dziedzicach, Grajewie, Gryfinie, Knurowie, Legionowie, Łomży, Myszkowie, Opocznie, Policach, Pszczynie, Sochaczewie, Śremie, Swarzędzu, Wałczu, Ząbkach i Zgorzelcu.

[100] Zakładka E-Urząd – Elektroniczne załatwianie spraw.

[101] UM w: Aleksandrowie Łódzkim, Augustowie, Białogardzie, Czechowicach-Dziedzicach, Grajewie, Gryfinie, Hajnówce, Knurowie, Koluszkach, Legionowie, Łomży, Myszkowie, Obornikach, Oleśnicy, Opocznie, Piastowie, Policach, Pszczynie, Sochaczewie, Śremie, Swarzędzu, Wolsztynie i Ząbkach.

w narzędziach informatycznych, tworzenie formularzy ePUAP, zagrożenia utraty danych i technicznych środków zapobiegania naruszeniom bezpieczeństwa informacji, sposoby postępowania pracowników zapobiegające naruszeniom oraz skutkom naruszenia bezpieczeństwa informacji łącznie z odpowiedzialnością prawną.

W pozostałych pięciu urzędach[102] nie zapewniono pełnych szkoleń pracowników w zakresie bezpieczeństwa informacji, co było niezgodne z § 20 ust. 2 pkt 6 rozporządzenia KRI. Prowadzone w tych urzędach szkolenia dotyczyły wyłącznie obsługi wdrożonych programów wspomagających procedurę obiegu dokumentów lub ochrony danych osobowych.

Ustanowienie i wdrożenie wewnętrznych procedur w zakresie bezpieczeństwa informacji

W 16 objętych kontrolą urzędach[103] (57%) brak było Systemu Zarządzania Bezpieczeństwem Informacji, o którym mowa w § 20 ust. 1 w związku z ust. 3 rozporządzenia KRI, w szczególności nie ustanowiono polityki bezpieczeństwa informacji. W myśl tego przepisu podmiot realizujący zadania publiczne opracowuje i ustanawia, wdraża i eksploatuje, monitoruje i przegląda oraz utrzymuje i doskonali system zarządzania bezpieczeństwem informacji zapewniający poufność, dostępność i integralność informacji z uwzględnieniem takich atrybutów, jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność. Ponadto § 20 ust. 3 rozporządzenia KRI wskazuje, że wymagania określone w ww. ust. 1 uznaje się za spełnione, jeżeli system zarządzania bezpieczeństwem informacji został opracowany na podstawie Polskiej Normy PN-ISO/IEC 27001[104], a ustanawianie zabezpieczeń, zarządzanie ryzykiem oraz audytowanie odbywa się na podstawie Polskich Norm związanych z tą normą[105]. W pkt 5.1 normy PN-EN ISO/IEC 27002[106] wskazano wymóg opracowania i stosowania dokumentu polityki bezpieczeństwa informacji.

Opracowane i wdrożone w tych jednostkach regulacje nie obejmowały wszystkich informacji jakie są przetwarzane w urzędzie[107], lecz dotyczyły głównie ochrony danych osobowych. Kontrolowani w wyjaśnieniach wskazywali m.in., że planowane są, bądź zostały podjęte prace dla przygotowania SZBI, w tym polityki bezpieczeństwa informacji.

---

[102] UM w: Oławie, Wałczu, Zelowie i Zgorzelcu, a także UG Długołęka.

[103] UM w: Aleksandrowie Łódzkim, Augustowie, Czechowicach-Dziedzicach, Grajewie, Koluszkach, Myszkowie, Obornikach, Oławie, Policach, Sochaczewie, Śremie, Swarzędzu, Wałczu, Zelowie i Zgorzelcu, a także UG Długołęka.

[104] Polska Norma PN-EN ISO/IEC 27001:2017 *Technika Informatyczna. Techniki bezpieczeństwa. Systemy zarządzania bezpieczeństwem informacji. Wymagania.*

[105] W tym: PN-ISO/IEC 27002 – w odniesieniu do ustanawiania zabezpieczeń, PN-ISO/IEC 27005 – w odniesieniu do zarządzania ryzykiem, PN-ISO/IEC 24762 – w odniesieniu do odtwarzania techniki informatycznej po katastrofie w ramach zarządzania ciągłością działania.

[106] Polska Norma PN-ISO/IEC 27002:2013 *Technika Informatyczna. Techniki bezpieczeństwa. Praktyczne zasady zabezpieczania informacji.*

[107] M.in. dotyczących konfiguracji infrastruktury informatycznej w tym serwerów, zarządzania hasłami dostępu do systemów IT, treści umów z dostawcami, warunków zastrzeżonych przez dostawców, tajemnic wynikających z innych aktów prawnych, jak np. prawa własności intelektualnej, zasad bezpieczeństwa fizycznego w obiekcie, korespondencji służbowej czy stosowanych zabezpieczeń systemów informatycznych.

Przykład

Burmistrz Augustowa wyjaśnił m.in., że: *Działania zmierzające do ustanowienia Polityki bezpieczeństwa informacji zostały rozpoczęte w 2019 r. Podjęto szereg czynności zmierzających do aktualizacji dokumentacji w zakresie ochrony danych osobowych, zapewnienie kompetentnej kadry oraz infrastruktury informatycznej. Pracownicy Urzędu zostali przeszkoleni w zakresie bezpieczeństwa informacji. (...) W 2020 r. w Planie szkoleń pracowników zostały ujęte szkolenia wewnętrzne pracowników w tym zakresie. Planowany audyt KRI miał wskazać niezgodności i zalecenia względem stosowanych rozwiązań w zakresie bezpieczeństwa informacji. Na ich podstawie planowano wdrożyć odpowiednie regulacje i procedury w nowej lokalizacji. Okres pandemii przesunął w czasie wykonanie audytu i wdrożenie powyższych rozwiązań.*

Pozostałe 12 urzędów[108] objętych badaniem (tj. 43%) opracowało i wdrożyło procedury regulujące politykę bezpieczeństwa informacji.

Posiadanie informacji o wykorzystywanych zasobach informatycznych

W myśl przepisu § 20 ust. 2 pkt 2 rozporządzenia KRI zarządzanie bezpieczeństwem informacji realizowane jest w szczególności w taki sposób aby wszystkie aktywa informatyczne zostały zidentyfikowane, a także powinien zostać sporządzony i być na bieżąco aktualizowany spis tych aktywów. Aktualna inwentaryzacja sprzętu informatycznego powinna zawierać m.in. informację o jego rodzaju i konfiguracji, przez co możliwe będzie szybkie odtworzenie infrastruktury i świadczenie usług przez urząd, np. na wypadek katastrofy lub innego zdarzenia losowego.

W 11 urzędach[109] (z 28, tj. 39%) stwierdzono nieprawidłowości w zakresie spełnienia wymogów określonych w § 20 ust. 2 pkt 2 rozporządzenia KRI. I tak, w siedmiu urzędach[110], w których wykorzystywano oprogramowanie do ewidencjonowania sprzętu i oprogramowania wraz z ich konfiguracją stwierdzono, że ewidencja była niepełna lub dane w niej zawarte były nierzetelne, a w czterech pozostałych urzędach[111] spis urządzeń informatycznych prowadzono w formie arkusza danych lub wykazów papierowych. **NIK wskazuje, że zakres informacji dostępnych w papierowym rejestrze zasobów informatycznych jest niewystarczający,** gdyż nie zawiera aktualnych, pełnych informacji o posiadanych zasobach informatycznych, w tym ich rodzaju i konfiguracji, a zatem nie będzie możliwe sprawne odtworzenie infrastruktury informatycznej w przypadku katastrofy lub innego zdarzenia losowego.

Zarządzanie uprawnieniami użytkowników w systemach informatycznych

W wyniku przeprowadzonego przez NIK w urzędach badania blokowania/odbierania dostępu do systemów informatycznych na próbie 441 pracowników, którzy zakończyli zatrudnienie w okresie objętym kontrolą, stwierdzono, że w dziewięciu urzędach[112] 59 byłym pracownikom (tj. 13% próby byłych pracowników objętych badaniem) ich konta nie zostały

[108] UM w: Białogardzie, Gryfinie, Hajnówce, Knurowie, Legionowie, Łomży, Oleśnicy, Opocznie, Piastowie, Pszczynie, Wolsztynie i Ząbkach.

[109] UM w: Czechowicach-Dziedzicach, Gryfinie, Hajnówce, Koluszkach, Myszkowie, Oleśnicy, Policach, Śremie, Wolsztynie, Zelowie, a także UG Długołęka.

[110] UM w: Gryfinie, Hajnówce, Koluszkach, Oleśnicy, Śremie, Wolsztynie, a także UG Długołęka.

[111] UM w: Czechowicach-Dziedzicach, Myszkowie, Policach, Zelowie.

[112] UM w (liczba osób): Czechowicach-Dziedzicach (12), Knurowie (4), Obornikach (3), Oleśnicy (3), Piastowie (11), Śremie (4), Wałczu (6) i Zelowie (14), a także UG Długołęka (2).

zablokowane i pozostawały wciąż aktywne. Było to niezgodne z § 20 ust. 2 pkt 5 rozporządzenia KRI, stanowiącym że zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienie przez kierownictwo podmiotu publicznego warunków umożliwiających realizację i egzekwowanie bezzwłocznej zmiany uprawnień, w przypadku zmiany zadań osób zaangażowanych w proces przetwarzania informacji. Zakres nieodebranych uprawnień, jak i okres po jakim zablokowano dostęp do kont był w poszczególnych urzędach zróżnicowany.

Przykład

W **Urzędzie Miasta Piastowa** nie stosowano się do wymogu bezzwłocznej zmiany uprawnień, w przypadku zmiany zadań osób. Z analizy terminów odebrania uprawnień poszczególnym pracownikom wynika, że w przypadku 11 (spośród 15 zbadanych spraw zakończenia zatrudnienia przez pracowników posiadających dostęp do systemu EZD lub FK) odebranie uprawnień do ww. systemów nastąpiło w okresie od 59 do 931 dni.

Zdaniem NIK, konieczne jest podejmowanie działań zapewniających, iż osoby zaangażowane w proces przetwarzania informacji posiadają stosowne uprawnienia i uczestniczą w tym procesie w stopniu adekwatnym do realizowanych przez nie zadań oraz obowiązków. NIK zwraca również uwagę na konieczność dokonywania bezzwłocznej zmiany uprawnień, bądź blokowania lub odbierania uprawnień, w przypadku zmiany zadań lub ustania zatrudnienia.

Ponadto w trakcie kontroli ustalono, że spośród 283 objętych badaniem pracowników wykonujących zadania w systemach informatycznych, 27 z nich (tj. 10%) miało możliwość zainstalowania na użytkowanych komputerach dowolnego oprogramowania. Osoby te nie były pracownikami służb informatycznych, mimo to posiadały uprawnienia administratora systemu na używanych przez siebie komputerach, w związku z czym mogły samodzielnie instalować dowolne oprogramowanie. Było to niezgodne z wymaganiami określonymi w § 20 ust. 2 pkt 4 rozporządzenia KRI, stanowiącym że zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienie przez kierownictwo podmiotu publicznego warunków umożliwiających realizację i egzekwowanie m.in. podejmowania działań zapewniających, że osoby zaangażowane w proces przetwarzania informacji posiadają stosowne uprawnienia i uczestniczą w tym procesie w stopniu adekwatnym do realizowanych przez nie zadań oraz obowiązków mających na celu zapewnienie bezpieczeństwa informacji. Sytuacja taka wystąpiła w sześciu urzędach[113] (z 28 kontrolowanych, tj. w 21%). W trakcie kontroli NIK, odbierano tym pracownikom uprawnienia administracyjne.

NIK wskazuje, że potrzeba ograniczania uprawnień w systemach informatycznych urzędów wynika także z konieczności ograniczenia ryzyka nieświadomego zainstalowania przez użytkownika złośliwego

[113] UM w (liczba badanych użytkowników/liczba użytkowników posiadających uprawnienia administratora): Augustowie (10/1), Obornikach (10/9), Oleśnicy (10/4), Policach (10/1), Wolsztynie (10/10), Zelowie (10/2).

oprogramowania np. w trakcie przeglądania stron internetowych. Oprogramowanie antywirusowe i inne wewnętrzne systemy zabezpieczające bez tego ograniczenia nie dają wystarczającej gwarancji bezpiecznej pracy w systemie informatycznym.

Audyty bezpieczeństwa informacji

W okresie objętym kontrolą nie przeprowadzono audytu w zakresie bezpieczeństwa informacji łącznie w 16 urzędach (tj. 57%), co było niezgodne z § 20 ust. 2 pkt 14 rozporządzenia KRI. Spośród 16 urzędów, w ośmiu[114] audyt nie został przeprowadzony w całym okresie objętym kontrolą, tj. w latach 2016–2019, natomiast w pozostałych ośmiu[115] urzędach audyt taki nie był przeprowadzany corocznie, lecz rzadziej.

W 12 jednostkach, w których przeprowadzono coroczny audyt bezpieczeństwa informacji, sformułowane zostały zalecenia-rekomendacje ukierunkowane na wzmocnienie bezpieczeństwa przetwarzania informacji i dotyczyły m.in.: stworzenia i wdrożenia planów rozwiązań ograniczających ryzyka (stworzenie sformalizowanych procedur), zabezpieczeń sieci wewnętrznej i zewnętrznej urzędu, nadawania pracownikom w systemach operacyjnych uprawnień adekwatnych do realizowanych zadań, aktualizacji informacji w zakresie inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji obejmujących ich rodzaj i konfigurację oraz monitorowania dostępu do informacji poprzez bieżącą analizę zapisów w dziennikach systemów. **Jako konieczne wskazywano również wsparcie ze strony kierownictwa w działaniach zapewniających bezpieczeństwo informacji urzędu i zasobów IT, jako infrastruktury krytycznej dla działań IT.**

[114] UM w: Czechowicach-Dziedzicach, Oleśnicy, Policach, Swarzędzu, Wałczu, Wolsztynie i Zgorzelcu, a także UG Długołęka.

[115] UM w: Aleksandrowie Łódzkim, Augustowie, Grajewie, Hajnówce, Koluszkach, Legionowie, Oławie i Zelowie.

6. ZAŁĄCZNIKI

6.1. Metodyka kontroli i informacje dodatkowe

Cel główny kontroli

Czy w celu świadczenia usług elektronicznych zapewniono sprawne działanie platformy ePUAP oraz podjęto działania na rzecz zwiększenia liczby usług elektronicznych i ich dostępności dla obywateli?

Cele szczegółowe

1. Czy Minister Cyfryzacji[116] podejmował skuteczne działania w celu zapewnienia dostępności i zwiększenia liczby e-usług dla obywateli?
2. Czy platforma ePUAP oraz profil zaufany funkcjonują w sposób umożliwiający sprawne i bezpieczne załatwianie spraw przez obywateli i urzędy administracji publicznej?
3. Czy urzędy j.s.t. świadczą e-usługi sprawnie i bezpiecznie?

Zakres podmiotowy

Kontrolą objęto 30 jednostek: Ministerstwo Cyfryzacji[117], Centralny Ośrodek Informatyki i 28 urzędów miast oraz gmin.

Kryteria kontroli

Kontrolę przeprowadzono na podstawie art. 2 ust. 1 (MC, COI) ustawy o NIK, z uwzględnieniem kryteriów: legalności, celowości, gospodarności i rzetelności i art. 2 ust. 2 (urzędy miast oraz gmin) ustawy o NIK, z uwzględnieniem kryteriów: legalności, gospodarności i rzetelności.

Okres objęty kontrolą

Kontrolą objęto okres od 1 stycznia 2016 r. do zakończenia czynności kontrolnych w danej jednostce. Czynności kontrolne przeprowadzono w okresie pomiędzy 25 maja 2020 r. a 5 listopada 2020 r. Ostatnie wystąpienie pokontrolne zostało wysłane 6 listopada 2020 r.

Zgłoszono dziesięć zastrzeżeń do jednego wystąpienia pokontrolnego, z czego dwa zostały uwzględnione w całości, dwa uwzględniono w części, a sześć oddalono.

Stan realizacji wniosków pokontrolnych

Do kierowników jednostek kontrolowanych zostało skierowanych 30 wystąpień pokontrolnych. Łącznie NIK sformułowała 105 wniosków pokontrolnych. Według stanu na dzień 25 stycznia 2021 r. zrealizowanych zostało 38 wniosków, 61 było w trakcie realizacji, a sześć było niezrealizowanych.

Wnioski NIK skierowane do burmistrzów/prezydentów miast dotyczyły m.in.:

- opracowania i wdrożenia systemu zarządzania bezpieczeństwem informacji, a w szczególności polityki bezpieczeństwa informacji;
- wprowadzenia procedur elektronicznego obiegu dokumentów oraz załatwiania spraw w formie elektronicznej w urzędzie;
- zapewnienia zamieszczenia na stronie internetowej urzędu informacji o możliwości załatwienia spraw drogą elektroniczną, w tym dotyczących Elektronicznej Skrzynki Podawczej ePUAP, listy spraw możliwych

[116] Minister Cyfryzacji kieruje działem administracji rządowej – informatyzacja. Zgodnie z rozporządzeniem Prezesa Rady Ministrów z dnia 6 października 2020 r. w sprawie szczegółowego zakresu działania Ministra Cyfryzacji (Dz. U. poz. 1716), jego obsługę zapewnia Kancelaria Prezesa Rady Ministrów.

[117] Rozporządzeniem Rady Ministrów z dnia 7 października 2020 r. (Dz. U. poz. 1730), z mocą od dnia 6 października 2020 r., zniesione zostało Ministerstwo Cyfryzacji, a pracownicy dotychczasowego Ministerstwa Cyfryzacji obsługujący sprawy działu informatyzacja zostali włączeni do Kancelarii Prezesa Rady Ministrów.

do załatwienia w formie e-usług oraz informacji o konieczności posiadania przez obywatela profilu zaufanego lub „nowego" dowodu osobistego z warstwą elektroniczną, w przypadku korzystania z e-usług;

– zapewnienia szkoleń pracownikom urzędu w zakresie bezpieczeństwa informacji;

– niezwłocznego blokowania dostępu i odbieranie uprawnień do systemów informatycznych pracownikom, którzy zakończyli zatrudnienie w urzędzie;

– zapewnienia prowadzenia przynajmniej raz w roku okresowego audytu wewnętrznego z zakresu bezpieczeństwa informacji.

Kierownicy kontrolowanych urzędów poinformowali o podjęciu działań na rzecz realizacji wniosków pokontrolnych.

W kontroli uczestniczyły: Departament Administracji Publicznej oraz sześć Delegatur NIK.

Wykaz jednostek kontrolowanych

Lp.	Jednostka organizacyjna NIK przeprowadzająca kontrolę	Nazwa jednostki kontrolowanej	Imię i nazwisko kierownika jednostki kontrolowanej
1.	Departament Administracji Publicznej	Ministerstwo Cyfryzacji	Mateusz Morawiecki powołany na urząd Ministra Cyfryzacji postanowieniem Prezydenta RP z dnia 6 października 2020 r.; Marek Zagórski (od 17 kwietnia 2018 r. do 6 października 2020 r.); od 9 stycznia 2018 r. do 16 kwietnia 2018 r. zastępstwo ministra właściwego do spraw informatyzacji sprawował Mateusz Morawiecki Prezes Rady Ministrów, który 11 stycznia 2018 r. upoważnił do wykonywania zadań Ministra Cyfryzacji Marka Zagórskiego, sekretarza stanu w Ministerstwie Cyfryzacji; Anna Streżyńska (od 16 listopada 2015 r. do 9 stycznia 2018 r.)
2.		Centralny Ośrodek Informatyki	Marcin Walentynowicz od 1 lutego 2018 r.; Marcin Suchar od 23 czerwca 2017r. do 31 stycznia 2018 r.; Monika Jakubiak od 1 września 2016r. do 23 czerwca 2017 r.; Rafał Leśkiewicz; od 1 czerwca 2016 r. do 31 sierpnia 2016 r.; Adam Sobczak od 27 stycznia 2016 r. do 31 maja 2016 r.; Nikodem Bończa-Tomaszewski od 19 kwietnia 2012 r. do 26 stycznia 2016 r.

Lp.	Jednostka organizacyjna NIK przeprowadzająca kontrolę	Nazwa jednostki kontrolowanej	Imię i nazwisko kierownika jednostki kontrolowanej
3.	Departament Administracji Publicznej	Urząd Miasta Legionowo	Roman Smogorzewski
4.		Urząd Miasta Piastowa	Grzegorz Szuplewski
5.		Urząd Miasta Sochaczewa	Piotr Osiecki
6.		Urząd Miasta Ząbki	Małgorzata Zyśk od 21 listopada 2018 r. Robert Perkowski od 6 grudnia 2006 r. do 20 listopada 2018 r.
1.	Delegatura NIK w Białymstoku	Urząd Miejski w Augustowie	Mirosław Korolczuk
2.		Urząd Miasta Grajewo	Dariusz Latarowski
3.		Urząd Miasta Hajnówka	Jerzy Sirak
4.		Urząd Miejski w Łomży	Mariusz Chrzanowski
1.	Delegatura NIK w Katowicach	Urząd Miejski w Czechowicach-Dziedzicach	Marian Błachut
2.		Urząd Miasta w Knurowie	Adam Rams
3.		Urząd Miasta Myszków	Włodzimierz Żak
4.		Urząd Miejski w Pszczynie	Dariusz Skrobol
1.	Delegatura NIK w Łodzi	Urząd Miejski w Aleksandrowie Łódzkim	Jacek Lipiński
2.		Urząd Miejski w Koluszkach	Waldemar Chałat
3.		Urząd Miejski w Opocznie	Dariusz Wojciech Kosno od 5 listopada 2018 r. Rafał Janusz Kądziela od 3 grudnia 2014 r. do 4 listopada 2018 r.
4.		Urząd Miejski w Zelowie	Tomasz Jachymek od 22 listopada 2018 r. Urszula Świerczyńska od 6 grudnia 2010 r. do 21 listopada 2018 r.
1.	Delegatura NIK w Poznaniu	Urząd Miejski w Obornikach	Tomasz Szrama
2.		Urząd Miasta i Gminy w Swarzędzu	Marian Szkudlarek
3.		Urząd Miejski w Śremie	Adam Lewandowski
4.		Urząd Miejski w Wolsztynie	Wojciech Lis

Lp.	Jednostka organizacyjna NIK przeprowadzająca kontrolę	Nazwa jednostki kontrolowanej	Imię i nazwisko kierownika jednostki kontrolowanej
1.	Delegatura NIK w Szczecinie	Urząd Miasta Białogard	Emilia Bury od 21 listopada 2018 r. Krzysztof Bagiński od 15 grudnia 2010 r.
2.		Urząd Miasta i Gminy w Gryfinie	Mieczysław Sawaryn
3.		Urząd Miejski w Policach	Władysław Diakun
4.		Urząd Miasta Wałcz	Maciej Żebrowski od 19 listopada 2018 r. Bogusława Towalewska od 9 grudnia 2014 r.
1.	Delegatura NIK we Wrocławiu	Urząd Gminy Długołęka	Wojciech Stanisław Błoński
2.		Urząd Miasta Oleśnicy	Jan Broń od 5 listopada 2018 r. Michał Kołaciński od 8 grudnia 2014 r. do 4 listopada 2018 r.
3.		Urząd Miejski w Oławie	Tomasz Frischmann
4.		Urząd Miasta Zgorzelec	Rafał Gronicz

Wykaz ocen kontrolowanych jednostek

L.p.	Nazwa jednostki kontrolowanej	Ocena kontrolowanej działalności*)	Stany mające wpływ na wydaną ocenę:	
			prawidłowe	nieprawidłowe
1.	Ministerstwo Cyfryzacji	w formie opisowej	Minister Cyfryzacji w latach 2016–2020 podejmował odpowiednie działania w celu zapewnienia dostępności i zwiększenia liczby e-usług dla obywateli.	Minister nie zapewnił przed zawarciem aneksu nr 4 do umowy dotyczącej m.in. utrzymania i rozwoju ePUAP, niezależnej oceny prawidłowości przygotowanego przez COI nowego kosztorysu do ww. umowy oraz nie udokumentował procesu negocjacji kosztów wynagrodzenia dla COI.

L.p.	Nazwa jednostki kontrolowanej	Ocena kontrolowanej działalności*)	Stany mające wpływ na wydaną ocenę:	
			prawidłowe	nieprawidłowe
2.	Centralny Ośrodek Informatyki	w formie opisowej	COI na zlecenie MC zapewnił utrzymanie i rozwój systemów ePUAP oraz PZ zgodnie z umowami.	Stwierdzone nieprawidłowości dotyczyły m.in.: - określenia w umowach na utrzymanie systemów ePUAP oraz PZ nierzetelnego mechanizmu pomiaru jakości obsługi zgłoszeń problemów przez użytkowników, a także zbyt długich maksymalnych czasów obsługi poszczególnych kategorii incydentów - niepełnego wdrożenia SZBI, - przeprowadzenia przez COI niekompletnych testów bezpieczeństwa systemów ePUAP i PZ.
3.	Urząd Miasta Legionowo	w formie opisowej	Wdrożone w Urzędzie zasady świadczenia e-usług umożliwiały ich sprawną i terminową realizację.	Stwierdzone nieprawidłowości dotyczyły m.in.: - braku regulacji dotyczących Polityki Bezpieczeństwa Informacji w okresie do 25 maja 2018 r. do 22 września 2020 r., - nieprzeprowadzeniu w 2017 r. i 2019 r. audytu z zakresu bezpieczeństwa informacji, - braku niezwłocznego odebrania uprawnień do systemów informatycznych, pracownikom którzy zakończyli pracę w Urzędzie.

L.p.	Nazwa jednostki kontrolowanej	Ocena kontrolowanej działalności*)	Stany mające wpływ na wydaną ocenę:	
			prawidłowe	nieprawidłowe
4.	Urząd Miasta Piastowa	w formie opisowej	Wdrożone w Urzędzie zasady świadczenia e-usług umożliwiały ich sprawną i terminową realizację. Ponadto wdrożono rozwiązania w zakresie bezpiecznego gromadzenia i przetwarzania danych.	Stwierdzone nieprawidłowości dotyczyły: - braku bezzwłocznego odbierania uprawnień do systemów pomimo zakończenia zatrudnienia w Urzędzie, - niezamieszczeniu na stronie Urzędu informacji o funkcjonalnościach nowego dowodu osobistego.
5.	Urząd Miasta Sochaczewa	w formie opisowej	Wdrożone w Urzędzie zasady świadczenia e-usług umożliwiały ich sprawną i terminową realizację.	Stwierdzone nieprawidłowości dotyczyły: - braku Systemu Zarządzania Bezpieczeństwem Informacji, - niezamieszczeniu na stronie Urzędu informacji o funkcjonalnościach nowego dowodu osobistego.
6.	Urząd Miasta Ząbki	pozytywna	Wdrożone w Urzędzie zasady świadczenia e-usług umożliwiały ich sprawną i terminową realizację. Ponadto wdrożono rozwiązania w zakresie bezpiecznego gromadzenia i przetwarzania danych.	

L.p.	Nazwa jednostki kontrolowanej	Ocena kontrolowanej działalności*)	Stany mające wpływ na wydaną ocenę:	
			prawidłowe	nieprawidłowe
7.	Urząd Miejski w Augustowie	w formie opisowej	Wdrożone w Urzędzie zasady świadczenia e-usług umożliwiały ich sprawną i terminową realizację.	Stwierdzone nieprawidłowości polegały na: - braku Systemu Zarządzania Bezpieczeństwem Informacji, - nie przeprowadzeniu w latach 2016–2017 i 2019–2020 (do 24 lipca) audytu z zakresu bezpieczeństwa informacji.
8.	Urząd Miasta Grajewo	w formie opisowej	Wdrożone w Urzędzie zasady świadczenia e-usług umożliwiały ich sprawną i terminową realizację.	Stwierdzone nieprawidłowości polegały na: - braku Systemu Zarządzania Bezpieczeństwem Informacji, - nie przeprowadzeniu corocznych audytów z zakresu bezpieczeństwa informacji.
9.	Urząd Miasta Hajnówka	w formie opisowej	Wdrożone w Urzędzie zasady świadczenia e-usług umożliwiały ich sprawną i terminową realizację.	Stwierdzone nieprawidłowości polegały mi.in. na: - braku czytelnych informacji o spełnieniu koniecznych warunków do skorzystania z e-usług, - nie dokonywaniu bieżącej aktualizacji danych użytkowanego sprzętu i oprogramowania, - nie przeprowadzaniu audytu z zakresu bezpieczeństwa informacji (do 30 października 2019 r.).

L.p.	Nazwa jednostki kontrolowanej	Ocena kontrolowanej działalności*)	Stany mające wpływ na wydaną ocenę:	
			prawidłowe	nieprawidłowe
10.	Urząd Miejski w Łomży	pozytywna	Wdrożone w Urzędzie zasady świadczenia e-usług umożliwiały ich sprawną i terminową realizację. Ponadto wdrożono rozwiązania w zakresie bezpiecznego gromadzenia i przetwarzania danych.	NIK nie stwierdziła nieprawidłowości.
11.	Urząd Miejski w Czechowicach-Dziedzicach	w formie opisowej	Wdrożone w Urzędzie zasady świadczenia e-usług umożliwiały ich sprawną i terminową realizację.	Stwierdzone nieprawidłowości polegały mi.in. na: - braku Systemu Zarządzania Bezpieczeństwem Informacji, - nie przeprowadzeniu corocznych audytów z zakresu bezpieczeństwa informacji. - odbieraniu/blokowaniu ze zwłoką (wynoszącą nawet 212 dni) kont dostępu do systemów informatycznych byłym pracownikom Urzędu.
12.	Urząd Miasta w Knurowie	w formie opisowej	Wdrożone w Urzędzie zasady świadczenia e-usług umożliwiały ich sprawną i terminową realizację. Ponadto wdrożono rozwiązania w zakresie bezpiecznego gromadzenia i przetwarzania danych.	Stwierdzona nieprawidłowość dotyczyła zwłoki w złożeniu przez kierowników komórek organizacyjnych czterech spośród 15 zbadanych wniosków o odebranie uprawnień dostępu pracownikom do sieci informatycznej Urzędu.

L.p.	Nazwa jednostki kontrolowanej	Ocena kontrolowanej działalności*)	Stany mające wpływ na wydaną ocenę:	
			prawidłowe	nieprawidłowe
13.	Urząd Miasta Myszków	w formie opisowej	Wdrożone w Urzędzie zasady świadczenia e-usług umożliwiały ich sprawną i terminową realizację.	Stwierdzone nieprawidłowości polegały mi.in. na: - braku Systemu Zarządzania Bezpieczeństwem Informacji, - nieprzeprowadzeniu corocznych audytów z zakresu bezpieczeństwa informacji. - nie prowadzeniu inwentaryzacji zasobów informatycznych.
14.	Urząd Miejski w Pszczynie	pozytywna	Wdrożone w Urzędzie zasady świadczenia e-usług umożliwiały ich sprawną i terminową realizację. Ponadto wdrożono rozwiązania w zakresie bezpiecznego gromadzenia i przetwarzania danych.	NIK nie stwierdziła nieprawidłowości.
15.	Urząd Miejski w Aleksandrowie Łódzkim	w formie opisowej	Wdrożone w Urzędzie zasady świadczenia e-usług umożliwiały ich sprawną i terminową realizację.	Stwierdzone nieprawidłowości polegały mi.in. na: - braku Systemu Zarządzania Bezpieczeństwem Informacji, - nieprzeprowadzeniu corocznych audytów z zakresu bezpieczeństwa informacji.

L.p.	Nazwa jednostki kontrolowanej	Ocena kontrolowanej działalności*)	Stany mające wpływ na wydaną ocenę:	
			prawidłowe	nieprawidłowe
16.	Urząd Miejski w Koluszkach	negatywna	Wdrożone w Urzędzie zasady świadczenia e-usług umożliwiały ich realizację.	Stwierdzone nieprawidłowości polegały mi.in. na: - nierzetelnym dokumentowaniu czynności w ramach prowadzonych spraw wpływających poprzez platformę ePUAP, - realizowaniu e-usług z opóźnieniem, - braku Systemu Zarządzania Bezpieczeństwem Informacji, - niezapewnieniu należytej i terminowej realizacji zadań dotyczących odbierania uprawnień do systemów informatycznych osobom, które zakończyły zatrudnienie w Urzędzie, - nieprzeprowadzeniu w 2016 r. i w 2018 r. audytu wewnętrznego w zakresie bezpieczeństwa informacji.
17.	Urząd Miejski w Opocznie	w formie opisowej	Wdrożone w Urzędzie zasady świadczenia e-usług umożliwiały ich sprawną i terminową realizację. Ponadto wdrożono rozwiązania w zakresie bezpiecznego gromadzenia i przetwarzania danych.	NIK nie stwierdziła nieprawidłowości.

L.p.	Nazwa jednostki kontrolowanej	Ocena kontrolowanej działalności*)	Stany mające wpływ na wydaną ocenę:	
			prawidłowe	nieprawidłowe
18.	Urząd Miejski w Zelowie	w formie opisowej	Wdrożone w Urzędzie zasady świadczenia e-usług umożliwiały ich sprawną i terminową realizację.	Stwierdzone nieprawidłowości polegały mi.in. na: - braku Systemu Zarządzania Bezpieczeństwem Informacji, - nie prowadzeniu audytów bezpieczeństwa informacji w latach 2018–2020, - niezapewnieniu należytej i terminowej realizacji zadań dotyczących odbierania uprawnień do systemów informatycznych osobom, które zakończyły zatrudnienie w Urzędzie.
19.	Urząd Miejski w Obornikach	w formie opisowej	Wdrożone w Urzędzie zasady świadczenia e-usług umożliwiały ich sprawną i terminową realizację.	Stwierdzone nieprawidłowości polegały mi.in. na: - braku Systemu Zarządzania Bezpieczeństwem Informacji, - posiadaniu przez użytkowników systemów informatycznych, niebędących pracownikami służb informatycznych uprawnień administracyjnych do komputerów, - niezapewnieniu należytej i terminowej realizacji zadań dotyczących odbierania uprawnień do systemów informatycznych osobom, które zakończyły zatrudnienie w Urzędzie.
20.	Urząd Miasta i Gminy w Swarzędzu	w formie opisowej	Wdrożone w Urzędzie zasady świadczenia e-usług umożliwiały ich sprawną i terminową realizację.	Stwierdzone nieprawidłowości polegały mi.in. na: - braku Systemu Zarządzania Bezpieczeństwem Informacji, - nieprzeprowadzaniu audytu wewnętrznego z zakresu bezpieczeństwa informacji.

L.p.	Nazwa jednostki kontrolowanej	Ocena kontrolowanej działalności*)	Stany mające wpływ na wydaną ocenę:	
			prawidłowe	nieprawidłowe
21.	Urząd Miejski w Śremie	w formie opisowej	Wdrożone w Urzędzie zasady świadczenia e-usług umożliwiały ich sprawną i terminową realizację.	Stwierdzone nieprawidłowości polegały mi.in. na: - braku Systemu Zarządzania Bezpieczeństwem Informacji, - niezapewnieniu należytej i terminowej realizacji zadań dotyczących odbierania uprawnień do systemów informatycznych osobom, które zakończyły zatrudnienie w Urzędzie.
22.	Urząd Miejski w Wolsztynie	w formie opisowej	Wdrożone w Urzędzie zasady świadczenia e-usług umożliwiały ich sprawną i terminową realizację.	Stwierdzone nieprawidłowości polegały mi.in. na: - niedostosowaniu zapisów Regulaminu Organizacyjnego Urzędu w zakresie możliwości składania skarg i wniosków drogą elektroniczną, - posiadaniu przez użytkowników systemów informatycznych, niebędących pracownikami służb informatycznych uprawnień administracyjnych do komputerów, - nieprzeprowadzaniu audytu wewnętrznego z zakresu bezpieczeństwa informacji.
23.	Urząd Miasta Białogard	w formie opisowej	Wdrożone w Urzędzie zasady świadczenia e-usług umożliwiały ich sprawną i terminową realizację. Ponadto wdrożono rozwiązania w zakresie bezpiecznego gromadzenia i przetwarzania danych.	NIK nie stwierdziła nieprawidłowości.

L.p.	Nazwa jednostki kontrolowanej	Ocena kontrolowanej działalności*)	Stany mające wpływ na wydaną ocenę:	
			prawidłowe	nieprawidłowe
24.	Urząd Miasta i Gminy w Gryfinie	w formie opisowej	Wdrożone w Urzędzie zasady świadczenia e-usług umożliwiały ich sprawną i terminową realizację.	Stwierdzone nieprawidłowości polegały mi.in. na: - nieopracowaniu procedur obiegu/zarządzania dokumentami, regulujących komunikację elektroniczną i załatwianie spraw w formie elektronicznej, - posiadaniu przez użytkowników systemów informatycznych, niebędących pracownikami służb informatycznych uprawnień administracyjnych do komputerów.
25.	Urząd Miejski w Policach	w formie opisowej	Wdrożone w Urzędzie zasady świadczenia e-usług umożliwiały ich sprawną i terminową realizację.	Stwierdzone nieprawidłowości polegały mi.in. na: - braku Systemu Zarządzania Bezpieczeństwem Informacji, - nieposiadaniu aktualnych informacji o zasobach informatycznych, - nieprzeprowadzaniu w latach 2016–2019 audytu wewnętrznego z zakresu bezpieczeństwa informacji.
26.	Urząd Miasta Wałcz	w formie opisowej	Wdrożone w Urzędzie zasady świadczenia e-usług umożliwiały ich sprawną i terminową realizację.	Stwierdzone nieprawidłowości polegały mi.in. na: - braku Systemu Zarządzania Bezpieczeństwem Informacji, - niezapewnieniu pełnych szkoleń pracowników w zakresie bezpieczeństwa informacji, - nieprzeprowadzaniu audytu wewnętrznego z zakresu bezpieczeństwa informacji.

L.p.	Nazwa jednostki kontrolowanej	Ocena kontrolowanej działalności*)	Stany mające wpływ na wydaną ocenę:	
			prawidłowe	nieprawidłowe
27.	Urząd Gminy Długołęka	w formie opisowej	Wdrożone w Urzędzie zasady świadczenia e-usług umożliwiały ich sprawną i terminową realizację.	Stwierdzone nieprawidłowości polegały mi.in. na: - braku Systemu Zarządzania Bezpieczeństwem Informacji, - nieposiadaniu aktualnych informacji o zasobach informatycznych, - niezapewnieniu pełnych szkoleń pracowników w zakresie bezpieczeństwa informacji.
28.	Urząd Miasta Oleśnicy	negatywna	Wdrożone w Urzędzie zasady świadczenia e-usług umożliwiały ich realizację.	Stwierdzone nieprawidłowości polegały mi.in. na: - braku Systemu Zarządzania Bezpieczeństwem Informacji, - niezapewnieniu cyklicznych szkoleń pracowników w zakresie bezpieczeństwa informacji, - niezapewnieniu należytej i terminowej realizacji zadań dotyczących odbierania uprawnień do systemów informatycznych osobom, które zakończyły zatrudnienie w Urzędzie, - przeprowadzaniu przez pracowników Urzędu bezpośrednio zaangażowanych w zapewnienie bezpieczeństwa informacji audytów wewnętrznych w tym zakresie, co naruszało zasady niezależności i obiektywności audytu.

L.p.	Nazwa jednostki kontrolowanej	Ocena kontrolowanej działalności*)	Stany mające wpływ na wydaną ocenę:	
			prawidłowe	nieprawidłowe
29.	Urząd Miejski w Oławie	w formie opisowej	Wdrożone w Urzędzie zasady świadczenia e-usług umożliwiały ich sprawną i terminową realizację.	Stwierdzone nieprawidłowości polegały mi.in. na: - braku Systemu Zarządzania Bezpieczeństwem Informacji, - nieprzeprowadzaniu w latach 2016–2017 audytu wewnętrznego z zakresu bezpieczeństwa informacji. - niezapewnieniu pełnych i cyklicznych szkoleń pracowników w zakresie bezpieczeństwa informacji.
30.	Urząd Miasta Zgorzelec	w formie opisowej	Wdrożone w Urzędzie zasady świadczenia e-usług umożliwiały ich sprawną i terminową realizację.	Stwierdzone nieprawidłowości polegały mi.in. na: - braku Systemu Zarządzania Bezpieczeństwem Informacji, - nieprzeprowadzaniu audytu wewnętrznego z zakresu bezpieczeństwa informacji. - niezapewnieniu pełnych szkoleń pracowników w zakresie bezpieczeństwa informacji.

*) pozytywna/negatywna/w formie opisowej

6.2. Analiza stanu prawnego i uwarunkowań organizacyjno-ekonomicznych

Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne[118]

Zgodnie z art. 16 ust. 1 ustawy o informatyzacji, podmioty publiczne organizując przetwarzanie danych w systemie teleinformatycznym, są obowiązane zapewnić możliwość przekazywania danych również w postaci elektronicznej przez wymianę dokumentów elektronicznych związanych z załatwianiem spraw należących do ich zakresu działania, wykorzystując informatyczne nośniki danych lub środki komunikacji elektronicznej.

Art. 16 ust. 1a ustawy o informatyzacji nakazuje podmiotom publicznym udostępnienie elektronicznej skrzynki podawczej (ESP) spełniającej standardy określone i opublikowane na ePUAP przez ministra właściwego do spraw informatyzacji oraz zapewnienie jej obsługi. W terminie 7 dni od dnia udostępnienia elektronicznej skrzynki podawczej, podmiot publiczny jest zobowiązany przekazać ministrowi ds. informatyzacji informację o jej adresie (art. 16 ust. 1b).

W art. 16 ust. 2 ustawy o informatyzacji określone zostały zasady prowadzenia przez podmioty publiczne wymiany informacji w postaci elektronicznej, obejmujące wykorzystanie wyłącznie systemów teleinformatycznych spełniających minimalne wymagania dla tych systemów (zdefiniowane w art. 3 pkt 9) oraz zapewnienie zgodności z minimalnymi wymaganiami dla rejestrów publicznych i wymiany informacji w postaci elektronicznej (zdefiniowanych w art. 3 pkt 10).

Na podstawie art. 16 ust. 3 ustawy o informatyzacji zostało wydane rozporządzenie Prezesa Rady Ministrów z dnia 14 września 2011 r. w sprawie sporządzania i doręczania dokumentów elektronicznych oraz udostępniania formularzy, wzorów i kopii dokumentów elektronicznych[118] (dalej: rozporządzenie w sprawie sporządzania i doręczania dokumentów elektronicznych).

W przypadku, gdy w przepisach prawa został wskazany organ właściwy do określenia wzoru dokumentu, jeżeli przepisy te nie wykluczają przesyłania dokumentów drogą elektroniczną, art. 16a ust. 1 ustawy o informatyzacji, nakłada na takie organy dwa obowiązki. Pierwszym jest przekazanie ministrowi ds. informatyzacji formularza (w terminie 3 miesięcy od wejścia w życie aktu ustanawiającego formularz) wraz z opisem usługi możliwej do zrealizowania z jego pomocą, w celu zamieszczenia formularza w centralnym repozytorium wzorów dokumentów, a opisu – w katalogu usług. Drugim obowiązkiem jest udostępnienie na ePUAP lub w innym systemie teleinformatycznym formularza elektronicznego umożliwiającego wygenerowanie dokumentu elektronicznego w celu złożenia go za pomocą środków komunikacji elektronicznej.

Zgodnie z art. 16b ust. 1 ustawy o informatyzacji, w przypadku gdy w przepisach prawa nie został wskazany organ właściwy do określenia wzoru dokumentu, wzór dokumentu elektronicznego może przekazać do centralnego repozytorium wzorów dokumentów elektronicznych organ, w któ-

[118] Dz. U. z 2018 r. poz. 180.

rego właściwości pozostają sprawy związane z określonym w tym wzorze zakresem użytkowym dokumentów elektronicznych, lub minister właściwy do spraw informatyzacji po zasięgnięciu w uzasadnionych przypadkach opinii organów, w których właściwości pozostają sprawy związane z określonym w tym wzorze zakresem użytkowym dokumentu elektronicznego.

Elektroniczna Platforma Usług Administracji Publicznej ePUAP

Zgodnie z art. 3 pkt 13 ustawy o informatyzacji, ePUAP to system teleinformatyczny, w którym instytucje publiczne udostępniają usługi przez pojedynczy punkt dostępowy w sieci Internet. Zapewnienie funkcjonowania ePUAP należy do obowiązków ministra właściwego do spraw informatyzacji (art. 19a ust. 1 ww. ustawy).

Zakres i warunki korzystania z elektronicznej platformy usług administracji publicznej, w tym dotyczące: zakładania konta i sposobu prowadzenia katalogu usług na ePUAP oraz warunków wymiany informacji między ePUAP a innymi systemami teleinformatycznymi zawarte zostały w rozporządzeniu Ministra Cyfryzacji z dnia 5 października 2016 r. w sprawie zakresu i warunków korzystania z elektronicznej platformy usług administracji publicznej[119]. Stosownie do § 9 ww. rozporządzenia, ePUAP udostępnia katalog usług zawierający informacje o usługach, a w szczególności: podstawę prawną usługi, nazwę usługi, nazwę usługodawcy, cel usługi, odbiorców usługi, kategorię usługi, umiejscowienie usługodawcy według podziału administracyjnego kraju. Stosownie do § 10 ust. 1 rozporządzenia ePUAP, podmioty publiczne do świadczenia usług w postaci elektronicznej mogą wykorzystywać w szczególności następujące funkcje ePUAP:

1) tworzenie i obsługa dokumentów elektronicznych przez osoby fizyczne i podmioty;
2) przesyłanie dokumentów elektronicznych;
3) wymiana danych między ePUAP a innymi systemami teleinformatycznymi;
4) identyfikacja użytkowników i rozliczalność ich działań;
5) weryfikacja podpisu elektronicznego;
6) tworzenie usług podmiotu publicznego lub usług kilku podmiotów publicznych współdziałających ze sobą, zbudowanych na podstawie dwóch lub więcej usług;
7) obsługa płatności elektronicznych;
8) działania związane z procesem potwierdzania profilu zaufanego;
9) weryfikacja zgodności dokumentu elektronicznego z jego wzorem określonym w centralnym repozytorium wzorów dokumentów elektronicznych;
10) wystawianie:
    a) urzędowego poświadczenia odbioru,
    b) elektronicznego poświadczenia opłaty,
    c) elektronicznego znacznika czasu

– z uwzględnieniem funkcjonalności ePUAP gwarantujących niezaprzeczalność tych poświadczeń.

[119] Dz. U. z 2019 r. poz. 1969.

Profil zaufany

Z dniem 11 września 2018 r. do ustawy o informatyzacji dodane zostały art. 20aa–20ae[120]. Zgodnie z art. 20aa ustawy o informatyzacji, minister właściwy do spraw informatyzacji odpowiada za funkcjonowanie systemu teleinformatycznego, który:

1) zapewnia obsługę publicznego systemu identyfikacji elektronicznej, w którym wydawany jest profil zaufany, a od 4 marca 2019 również profil osobisty[121];
2) umożliwia podmiotom publicznym:
   a) uwierzytelnienie osoby fizycznej przy użyciu środka identyfikacji elektronicznej, o którym mowa w pkt 1,
   b) zapewnienie osobie fizycznej możliwości opatrzenia dokumentu elektronicznego podpisem zaufanym.

Kompetencje Ministra Cyfryzacji związane z zarządzaniem publicznym systemem identyfikacji elektronicznej zostały określone w art. 20ab ustawy o informatyzacji, zgodnie z którym minister ds. informatyzacji:

1) zarządza publicznym systemem identyfikacji elektronicznej;
2) zapisuje i zachowuje informacje związane z zapewnieniem rozliczalności i niezaprzeczalności działań użytkownika korzystającego ze środka identyfikacji elektronicznej wydanego w publicznym systemie identyfikacji elektronicznej.

Art. 20ac ustawy o informatyzacji stanowi, że Minister Cyfryzacji jest administratorem danych przetwarzanych w systemie, o którym mowa w art. 20aa, oraz jakie dane mogą być przetwarzane się w tym systemie.

Zgodnie z art. 20ad ust. 1 ustawy o informatyzacji, profil zaufany zawiera dane identyfikujące osobę fizyczną obejmujące: imię (imiona), nazwisko, datę urodzenia, numer PESEL. W procedurze potwierdzania profilu zaufanego dane te są weryfikowane automatycznie z danymi zawartymi w rejestrze PESEL (art. 20ad ust. 2). W przypadku zmiany w rejestrze PESEL danych jest dokonywana automatyczna aktualizacja tych danych zawartych w profilu zaufanym (art. 20ad ust. 3), a aktualizacja danych zawartych w profilu zaufanym nie powoduje unieważnienia profilu zaufanego (art. 20ad ust. 4). Natomiast w przypadku gdy w rejestrze PESEL został odnotowany zgon osoby posiadającej profil zaufany, profil zaufany tej osoby jest automatycznie unieważniany (art. 20ad ust. 4a). Profil zaufany może zawierać także inne dane niż wymienione w ust. 1, w szczególności identyfikator oraz dane wykorzystywane w procesach uwierzytelniania i autoryzacji realizowanych przy użyciu profilu zaufanego (art. 20ad ust. 5).

W myśl art. 20ae ustawy o informatyzacji, podpis zaufany wywołuje skutki prawne, jeżeli został utworzony lub złożony w okresie ważności środka identyfikacji elektronicznej, o którym mowa w art. 20aa pkt 1. Dane w postaci elektronicznej opatrzone podpisem zaufanym są równoważne pod względem skutków prawnych dokumentowi opatrzonemu podpisem własnoręcznym, chyba że przepisy odrębne stanowią inaczej. Nie można

[120] Na mocy art. 29 pkt 10 ustawy z dnia 5 lipca 2018 r. o zmianie ustawy o usługach zaufania oraz identyfikacji elektronicznej oraz niektórych innych ustaw (Dz. U. poz. 1544, ze zm.).

[121] Art. 20aa pkt 1 ustawy o informatyzacji został zmieniony przez art. 23 pkt 2 ustawy z dnia 6 grudnia 2018 r. (Dz. U. z 2019 r. poz. 60) zmieniającej nin. ustawę z dniem 4 marca 2019 r.

odmówić ważności i skuteczności podpisowi zaufanemu tylko na tej podstawie, że istnieje w postaci elektronicznej.

Przed 11 września 2018 r. moc prawną profilu zaufanego regulował art. 20b[122] ustawy o informatyzacji, który stanowił, że podpis potwierdzony profilem zaufanym ePUAP wywołuje skutki prawne, jeżeli został utworzony lub złożony w okresie ważności tego profilu, a dane w postaci elektronicznej opatrzone podpisem potwierdzonym profilem zaufanym ePUAP są równoważne pod względem skutków prawnych dokumentowi opatrzonemu podpisem własnoręcznym (chyba, że przepisy odrębne stanowią inaczej).

Stosownie do art. 20c ust. 1 ustawy o informatyzacji, potwierdzenia profilu zaufanego, które polega na weryfikacji zgodności danych zawartych we wniosku o jego wydanie ze stanem faktycznym, oraz unieważnienia profilu zaufanego dokonuje:

1) punkt potwierdzający profil zaufany,
2) samodzielnie osoba fizyczna przy wykorzystaniu kwalifikowanego podpisu elektronicznego, w przypadku gdy kwalifikowany certyfikat podpisu elektronicznego zawiera dane obejmujące co najmniej: imię (imiona), nazwisko, PESEL;
3) samodzielnie osoba fizyczna przy nieodpłatnym wykorzystaniu środka identyfikacji elektronicznej stosowanego do uwierzytelniania w systemie teleinformatycznym banku krajowego lub innego przedsiębiorcy spełniającym warunki, o których mowa w art. 20d pkt 1, o ile środek ten potwierdza dane obejmujące co najmniej: imię (imiona), nazwisko, PESEL;
4) samodzielnie osoba fizyczna przy wykorzystaniu profilu osobistego.

Funkcję punktu potwierdzającego pełni: konsul, naczelnik urzędu skarbowego, wojewoda, Zakład Ubezpieczeń Społecznych, Narodowy Fundusz Zdrowia (art. 20c ust. 2 ustawy o informatyzacji). Funkcję punktu potwierdzającego, za zgodą ministra właściwego do spraw informatyzacji, mogą również pełnić inne podmioty wymienione w art. 20c ust. 3 ustawy o informatyzacji.

Tymczasowy profil zaufany

Tymczasowy profil zaufany to rozwiązanie wprowadzone na podstawie art. 33 pkt 2 ustawy z dnia 31 marca 2020 r. o zmianie ustawy o szczególnych rozwiązaniach związanych z zapobieganiem, przeciwdziałaniem i zwalczaniem COVID-19, innych chorób zakaźnych oraz wywołanych nimi sytuacji kryzysowych oraz niektórych innych ustaw[123]. Zgodnie z tym przepisem w ustawie o informatyzacji dodano art. 20ca w następującym brzmieniu:

1. Minister właściwy do spraw informatyzacji może udostępnić usługę online służącą do potwierdzania profilu zaufanego o krótszym okresie ważności, zwanego dalej „tymczasowym profilem zaufanym".
2. Okres ważności tymczasowego profilu zaufanego wynosi 3 miesiące.

[122] Uchylony przez art. 29 pkt 11 ustawy z dnia 5 lipca 2018 r. o zmianie ustawy o usługach zaufania oraz identyfikacji elektronicznej oraz niektórych innych ustaw.

[123] Dz.U. poz. 568, ze zm. Rozwiązanie to weszło w życie z dniem 31 marca 2020 r.

3. Minister właściwy do spraw informatyzacji może wydłużyć okres ważności tymczasowych profili zaufanych, uwzględniając szczególne okoliczności.
4. Minister właściwy do spraw informatyzacji udostępnia informację o przedłużeniu ważności tymczasowych profili zaufanych na swojej stronie podmiotowej w Biuletynie Informacji Publicznej.
5. Minister właściwy do spraw informatyzacji w celu potwierdzenia tożsamości osoby wnioskującej o potwierdzenie tymczasowego profilu zaufanego:
   1) przeprowadza wideoidentyfikację wnioskodawcy polegającą na:
      a) porównaniu wizerunku wnioskodawcy udostępnianego przez niego w czasie rzeczywistym za pośrednictwem transmisji audiowizualnej z wizerunkiem tego wnioskodawcy pobranym z Rejestru Dowodów Osobistych, o którym mowa w ustawie z dnia 6 sierpnia 2010 r. o dowodach osobistych, oraz
      b) weryfikacji danych zawartych w warstwie graficznej dowodu osobistego albo paszportu wnioskodawcy okazanego przez niego w czasie rzeczywistym za pośrednictwem transmisji audiowizualnej[124], oraz
      c) w uzasadnionych przypadkach – weryfikacji wiedzy wnioskodawcy przy wykorzystaniu danych dotyczących wnioskodawcy zgromadzonych w rejestrach publicznych lub w systemach teleinformatycznych, albo
   2) umożliwia wnioskodawcy wykorzystanie środka identyfikacji elektronicznej, wydanego przez podmiot publiczny.
6. Warunki organizacyjno-techniczne wymiany danych pomiędzy systemem teleinformatycznym, o którym mowa w art. 20aa pkt 1, a systemem teleinformatycznym, w którym wydawany jest środek identyfikacji elektronicznej, o którym mowa w ust. 5 pkt 2, ustalane są między ministrem właściwym do spraw informatyzacji a podmiotem publicznym odpowiedzialnym za ten system.
7. Minister właściwy do spraw informatyzacji sporządza nagranie audiowizualne z transmisji, o której mowa w ust. 5 pkt 1, i przechowuje je przez okres 6 lat[125].
8. Minister właściwy do spraw informatyzacji zapisuje w systemie, o którym mowa w art. 20aa pkt 1, informacje dotyczące środka identyfikacji elektronicznej, o którym mowa w ust. 5 pkt 2.

Podpis elektroniczny

Zgodnie z definicją zawartą w art. 3 pkt 12 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 uchylające dyrektywę 1999/93/WE[126] (dalej: rozporządzenie eIDAS), kwalifikowany podpis elektroniczny oznacza podpis elektroniczny, który: jest unikalnie przyporządkowany podpisującemu; umożliwia ustalenie tożsamości podpisują-

[124] Zmieniony z dniem 18 kwietnia 2020 r.

[125] Zmieniony z dniem 18 kwietnia 2020 r.

[126] Dz. Urz. UE L 257 z 28.08.2014, s. 73, ze zm.

cego; jest składany przy użyciu danych służących do składania podpisu elektronicznego, których podpisujący może, z dużą dozą pewności, użyć pod wyłączną swoją kontrolą; jest powiązany z danymi podpisanymi w taki sposób, że każda późniejsza zmiana danych jest rozpoznawalna[127]; jest składany za pomocą kwalifikowanego urządzenia do składania podpisu elektronicznego i który opiera się na kwalifikowanym certyfikacie podpisu elektronicznego. Zgodnie z art. 25 ust. 2 tego rozporządzenia, kwalifikowany podpis elektroniczny ma skutek prawny równoważny podpisowi własnoręcznemu.

Zgodnie z art. 14 ustawy z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej[128], kwalifikowany dostawca usług zaufania, wydając kwalifikowany certyfikat podpisu elektronicznego, jest obowiązany:

1) uzyskać od osoby ubiegającej się o certyfikat potwierdzenie przyporządkowania do niej danych służących do weryfikacji podpisu elektronicznego, które są zawarte w wydanym certyfikacie;
2) poinformować osobę ubiegającą się o certyfikat o procedurze zgłaszania żądań unieważnienia kwalifikowanego certyfikatu.

Dowody osobiste z warstwą elektroniczną

Nowelizacja z grudnia 2018 r.[129] wprowadziła z dniem 4 marca 2019 r. do ustawy z dnia 6 sierpnia 2010 r. o dowodach osobistych[130] m.in. art. 10a oraz 12a–12j, umożliwiające wydawanie nowych dowodów osobistych z elektroniczną warstwą, zwanych e-dowodami. Stosownie do art. 10a ust. 1 i 3 ustawy o dowodach osobistych, dowód osobisty posiadający warstwę graficzną i warstwę elektroniczną, umożliwia jego posiadaczowi: uwierzytelnianie w usługach online za pomocą profilu osobistego; składanie podpisu osobistego; potwierdzanie obecności w określonym czasie i miejscu.

Definicja podpisu osobistego została zawarta w art. 2 ust. 1 pkt 9 ustawy o dowodach osobistych, zgodnie z którym podpis osobisty to zaawansowany podpis elektroniczny w rozumieniu art. 3 pkt 11 rozporządzenia eIDAS, weryfikowany za pomocą certyfikatu podpisu osobistego. Profil osobisty oznacza zaś środek identyfikacji elektronicznej zawierający dane potwierdzane przez certyfikat identyfikacji i uwierzytelnienia (art. 2 ust. 1 pkt 10 ww. ustawy).

Zgodnie z art. 12a ust. 1 ustawy o dowodach osobistych, warstwa elektroniczna dowodu osobistego zawiera:

1) dane zamieszczone w warstwie graficznej dowodu osobistego zapisane w postaci elektronicznej wraz z danymi je uwierzytelniającymi, z wyjątkiem numeru CAN;
2) certyfikat identyfikacji i uwierzytelnienia wraz z danymi umożliwiającymi identyfikację elektroniczną i uwierzytelnienie;
3) certyfikat podpisu osobistego wraz z danymi do składania podpisu;

[127] Art. 26 w zw. z art. 3 pkt 11 rozporządzenia eIDAS.

[128] Dz. U. z 2020 r. poz. 1173.

[129] Ustawa z dnia 6 grudnia 2018 r. o zmianie ustawy o dowodach osobistych oraz niektórych innych ustaw (Dz. U. z 2019 r. poz. 60, ze zm.).

[130] Dz. U. z 2020 r. poz. 332, ze zm.

4) certyfikat potwierdzenia obecności wraz z danymi umożliwiającymi jego użycie;
5) przestrzeń umożliwiającą umożliwiająca zamieszczenie kwalifikowanego certyfikatu podpisu elektronicznego zgodnego z art. 28 rozporządzenia eIDAS.

Certyfikat identyfikacji i uwierzytelnienia jest zamieszczany w dowodach osobistych osób posiadających pełną zdolność do czynności prawnych oraz osób posiadających ograniczoną zdolność do czynności prawnych (art. 12a ust. 2 ustawy o dowodach osobistych). Certyfikat podpisu osobistego będą posiadały dowody osobiste wydane osobom, które posiadają pełną zdolność do czynności prawnych i przy składaniu wniosku o wydanie dowodu osobistego wyraziły zgodę na zamieszczenie tego certyfikatu, oraz osobom małoletnim, które ukończyły 13 rok życia, jeżeli rodzic, opiekun prawny lub kurator tej osoby przy składaniu wniosku o wydanie dowodu osobistego wyraził zgodę na zamieszczenie tego certyfikatu (art. 12a ust. 3 ustawy o dowodach osobistych). Certyfikat podpisu osobistego będzie więc zamieszczany w dowodzie osobistym osób, które będą chciały korzystać z tej funkcjonalności.

Zgodnie z art. 12d ustawy o dowodach osobistych, opatrzenie danych podpisem osobistym wywołuje w stosunku do podmiotu publicznego skutek prawny równoważny podpisowi własnoręcznemu. Skutek taki w stosunku do podmiotu innego niż podmiot publiczny, opatrzenie danych podpisem osobistym wywołuje jeżeli obie strony wyrażą na to zgodę.

Dokumenty elektroniczne – doręczanie i przechowywanie

Warunki organizacyjno-techniczne doręczania dokumentów elektronicznych określono w rozporządzeniu w sprawie sporządzania i doręczania dokumentów elektronicznych. Zgodnie z § 3 ust. 1 tego rozporządzenia, podmioty publiczne informują na swoich stronach podmiotowych BIP m.in. o:

- udostępnionym adresie elektronicznej skrzynki podawczej, podanym w formie identyfikatora URI (pkt 1);
- maksymalnym rozmiarze dokumentu elektronicznego wraz z załącznikami, wyrażonym w megabajtach, możliwym do doręczenia za pomocą elektronicznej skrzynki podawczej, nie mniejszym niż 5 megabajtów (pkt 2);
- zakresach użytkowych dokumentów elektronicznych tworzonych na podstawie wzorów umieszczonych przez te podmioty w centralnym repozytorium lub repozytorium wzorów dokumentów elektronicznych, o których mowa w art. 19b ust. 5 ustawy o informatyzacji (pkt 3);
- rodzajach informatycznych nośników danych, na których może zostać im doręczony dokument elektroniczny (pkt 4);
- rodzajach informatycznych nośników danych, na których może zostać zapisane urzędowe poświadczenie odbioru (pkt 5).

System teleinformatyczny służący do obsługi doręczeń zapewnia oznaczanie doręczonych dokumentów elektronicznych danymi stwierdzającymi ważność podpisów elektronicznych w momencie ich złożenia i czas ich weryfikacji (§ 5 rozporządzeniu w sprawie sporządzania i doręczania dokumentów elektronicznych).

W rozporządzeniu Ministra Spraw Wewnętrznych i Administracji z dnia 30 października 2006 r. w sprawie szczegółowego sposobu postępowania z dokumentami elektronicznymi[131] określono sposób postępowania z dokumentami elektronicznymi powstającymi w organach państwowych i państwowych jednostkach organizacyjnych, w organach jednostek samorządu terytorialnego i samorządowych jednostkach organizacyjnych oraz napływającymi do nich, a także zawarto:

– zasady ewidencjonowania, przechowywania, klasyfikowania i kwalifikowania dokumentów elektronicznych oraz ich zabezpieczania przed utratą i nieuprawnionymi zmianami oraz
– zasady i tryb brakowania dokumentacji niearchiwalnej oraz zasady i tryb przekazywania materiałów archiwalnych do archiwów państwowych.

Bezpieczeństwo informacji

Zgodnie z art. 13 ust. 1 ustawy o informatyzacji, podmiot publiczny używa do realizacji zadań publicznych systemów teleinformatycznych spełniających minimalne wymagania dla systemów teleinformatycznych oraz zapewniających interoperacyjność systemów na zasadach określonych w Krajowych Ramach Interoperacyjności.

W myśl § 15 ust. 1 rozporządzenia KRI, systemy teleinformatyczne używane przez podmioty realizujące zadania publiczne projektuje się, wdraża oraz eksploatuje z uwzględnieniem ich funkcjonalności, niezawodności, używalności, wydajności, przenoszalności i pielęgnowalności, przy zastosowaniu norm oraz uznanych w obrocie profesjonalnym standardów i metodyk.

Zarządzanie usługami realizowanymi przez systemy teleinformatyczne ma na celu dostarczanie tych usług na deklarowanym poziomie dostępności i odbywa się w oparciu o udokumentowane procedury (§ 15 ust. 2 rozporządzenia KRI). Wymagania określone w ust. 1 i 2 uznaje się za spełnione, jeśli projektowanie, wdrażanie, eksploatowanie, monitorowanie, przeglądanie, utrzymanie i udoskonalanie zarządzania usługą podmiotu realizującego zadanie publiczne odbywają się z uwzględnieniem Polskich Norm: PN-ISO/IEC 20000-1 i PN-ISO/IEC 20000-2 (§ 15 ust. 3 rozporządzenia KRI).

Zgodnie z załącznikiem nr 2 do rozporządzenia KRI, system teleinformatyczny używany do realizacji zadań publicznych musi obsługiwać standardy zapewniające dostęp do zasobów informacji oraz formaty danych określone w załączniku.

Podmiot realizujący zadania publiczne opracowuje i ustanawia, wdraża i eksploatuje, monitoruje i przegląda oraz utrzymuje i doskonali system zarządzania bezpieczeństwem informacji zapewniający poufność, dostępność i integralność informacji z uwzględnieniem takich atrybutów, jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność (§ 20 ust. 1 rozporządzenia KRI).

Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności poprzez zapewnienie przez kierownictwo podmiotu publicznego warun-

[131] Dz. U. Nr 206, poz. 1518.

ków umożliwiających realizację i egzekwowanie działań wymienionych w § 20 ust. 2 rozporządzenia KRI w zakresie:

1) zapewnienia aktualizacji regulacji wewnętrznych w zakresie dotyczącym zmieniającego się otoczenia;
2) utrzymywania aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji obejmującej ich rodzaj i konfigurację;
3) przeprowadzania okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji oraz podejmowania działań minimalizujących to ryzyko, stosownie do wyników przeprowadzonej analizy;
4) podejmowania działań zapewniających, że osoby zaangażowane w proces przetwarzania informacji posiadają stosowne uprawnienia i uczestniczą w tym procesie w stopniu adekwatnym do realizowanych przez nie zadań oraz obowiązków mających na celu zapewnienie bezpieczeństwa informacji;
5) bezzwłocznej zmiany uprawnień, w przypadku zmiany zadań osób, o których mowa w pkt 4;
6) zapewnienia szkolenia osób zaangażowanych w proces przetwarzania informacji ze szczególnym uwzględnieniem takich zagadnień, jak:
   a) zagrożenia bezpieczeństwa informacji,
   b) skutki naruszenia zasad bezpieczeństwa informacji, w tym odpowiedzialność prawna,
   c) stosowanie środków zapewniających bezpieczeństwo informacji, w tym urządzenia i oprogramowanie minimalizujące ryzyko błędów ludzkich;
7) zapewnienia ochrony przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami, przez:
   a) monitorowanie dostępu do informacji,
   b) czynności zmierzające do wykrycia nieautoryzowanych działań związanych z przetwarzaniem informacji,
   c) zapewnienie środków uniemożliwiających nieautoryzowany dostęp na poziomie systemów operacyjnych, usług sieciowych i aplikacji;
8) ustanowienia podstawowych zasad gwarantujących bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość;
9) zabezpieczenia informacji w sposób uniemożliwiający nieuprawnionemu jej ujawnienie, modyfikacje, usunięcie lub zniszczenie;
10) zawierania w umowach serwisowych podpisanych ze stronami trzecimi zapisów gwarantujących odpowiedni poziom bezpieczeństwa informacji;
11) ustalenia zasad postępowania z informacjami, zapewniających minimalizację wystąpienia ryzyka kradzieży informacji i środków przetwarzania informacji, w tym urządzeń mobilnych;
12) zapewnienia odpowiedniego poziomu bezpieczeństwa w systemach teleinformatycznych, polegającego w szczególności na:
   a) dbałości o aktualizację oprogramowania,
   b) minimalizowaniu ryzyka utraty informacji w wyniku awarii,
   c) ochronie przed błędami, utratą, nieuprawnioną modyfikacją,
   d) stosowaniu mechanizmów kryptograficznych w sposób adekwatny do zagrożeń lub wymogów przepisu prawa,
   e) zapewnieniu bezpieczeństwa plików systemowych,

f) redukcji ryzyk wynikających z wykorzystania opublikowanych podatności technicznych systemów teleinformatycznych,
g) niezwłocznym podejmowaniu działań po dostrzeżeniu nieujawnionych podatności systemów teleinformatycznych na możliwość naruszenia bezpieczeństwa,
h) kontroli zgodności systemów teleinformatycznych z odpowiednimi normami i politykami bezpieczeństwa;

13) bezzwłocznego zgłaszania incydentów naruszenia bezpieczeństwa informacji w określony i z góry ustalony sposób, umożliwiający szybkie podjęcie działań korygujących;
14) zapewnienia okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji, nie rzadziej niż raz na rok.

Zgodnie z § 20 ust. 3 rozporządzenia KRI, obowiązki, o których mowa w § 20 ust. 1 i 2 uznaje się za spełnione, jeżeli system zarządzania bezpieczeństwem informacji został opracowany na podstawie Polskiej Normy PN-ISO/IEC 27001, a ustanawianie zabezpieczeń, zarządzanie ryzykiem oraz audytowanie odbywa się na podstawie Polskich Norm związanych z tą normą, w tym: PN-ISO/IEC 27002 – w odniesieniu do ustanawiania zabezpieczeń; PN-ISO/IEC 27005 – w odniesieniu do zarządzania ryzykiem; PN-ISO/IEC 24762 – w odniesieniu do odtwarzania techniki informatycznej po katastrofie w ramach zarządzania ciągłością działania.

6.3. Wykaz aktów prawnych dotyczących kontrolowanej działalności

1. Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne[132].
2. Ustawa z dnia 31 marca 2020 r. o zmianie ustawy o szczególnych rozwiązaniach związanych z zapobieganiem, przeciwdziałaniem i zwalczaniem COVID-19, innych chorób zakaźnych oraz wywołanych nimi sytuacji kryzysowych oraz niektórych innych ustaw[133].
3. Ustawa z dnia 6 sierpnia 2010 r. o dowodach osobistych[134].
4. Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych[135].
5. Rozporządzenie Prezesa Rady Ministrów z dnia 14 września 2011 r. w sprawie sporządzania i doręczania dokumentów elektronicznych oraz udostępniania formularzy, wzorów i kopii dokumentów elektronicznych[136].
6. Rozporządzenie Ministra Cyfryzacji z dnia 5 października 2016 r. w sprawie zakresu i warunków korzystania z elektronicznej platformy usług administracji publicznej[137].
7. Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 30 października 2006 r. w sprawie szczegółowego sposobu postępowania z dokumentami elektronicznymi[138].
8. Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE[139].

[132] Dz. U. z 2020 r. poz. 346, ze zm.
[133] Dz. U. poz. 568, ze zm.
[134] Dz. U. z 2020 r. poz. 332, ze zm.
[135] Dz. U. z 2017 r. poz. 2247.
[136] Dz. U. z 2018 r. poz. 180.
[137] Dz. U. z 2019 r. poz. 1969.
[138] Dz. U. Nr 206, poz. 1518.
[139] Dz. Urz. UE L 257 z 28.08.2014, s. 73, ze zm.

6.4. Wykaz podmiotów, którym przekazano informację o wynikach kontroli

1. Prezydent Rzeczypospolitej Polskiej
2. Marszałek Sejmu Rzeczypospolitej Polskiej
3. Marszałek Senatu Rzeczypospolitej Polskiej
4. Prezes Rady Ministrów, Minister Cyfryzacji
5. Prezes Trybunału Konstytucyjnego
6. Rzecznik Praw Obywatelskich
7. Sejmowa Komisja Cyfryzacji, Innowacyjności i Nowoczesnych Technologii
8. Sejmowa Komisja do Spraw Kontroli Państwowej
9. Sejmowa Komisja Samorządu Terytorialnego i Polityki Regionalnej
10. Senacka Komisja Samorządu Terytorialnego i Administracji Państwowej
11. Prezydenci miast/burmistrzowie/wójtowie