KAP.430.016.2016
Nr ewid. 208/2016/P/16/006/KAP

Informacja o wynikach kontroli

SYSTEM REJESTRÓW PAŃSTWOWYCH – BEZPIECZEŃSTWO, FUNKCJONOWANIE I UŻYTECZNOŚĆ

DEPARTAMENT
ADMINISTRACJI PUBLICZNEJ

MISJĄ

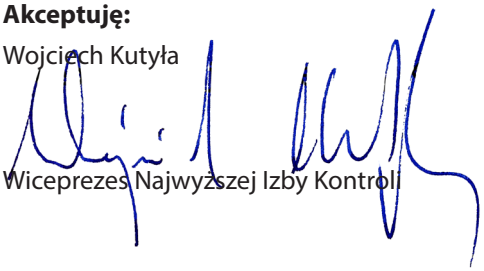
Najwyższej Izby Kontroli jest dbałość o gospodarność i skuteczność w służbie publicznej dla Rzeczypospolitej Polskiej

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

Dyrektor Departamentu Administracji Publicznej:
Bogdan Skwarka

Akceptuję:
Wojciech Kutyła



Wiceprezes Najwyższej Izby Kontroli

Zatwierdzam:
Krzysztof Kwiatkowski

Prezes Najwyższej Izby Kontroli
dnia 27.02.17 r.

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

www.nik.gov.pl

Spis treści

Zdjęcie na okładce:
Roter Würfel auf Tastatur mit FAQ - Frage Antwort: © Falko Müller - Riesa – Fotolia.com

Wykaz stosowanych skrótów, skrótowców i pojęć

akt stanu cywilnego	wpis o urodzeniu, małżeństwie lub zgonie w rejestrze stanu cywilnego wraz z treścią późniejszych wpisów wpływających na treść lub ważność tego aktu[1];
aplikacje wspierające	niezależne od aplikacji „Źródło" oprogramowanie wykorzystywane w Urzędach Stanu Cywilnego,
aplikacja „Źródło"	program do przetwarzania danych gromadzonych w Systemie Rejestrów Państwowych. Aplikacja została udostępniona urzędom miast/miast i gmin/gmin realizującym zadania z wykorzystaniem Systemu Rejestrów Państwowych;
BUSC	Baza Usług Stanu Cywilnego, jeden z modułów aplikacji „Źródło", za pomocą którego następuje obsługa Rejestru Stanu Cywilnego;
COI	Centralny Ośrodek Informatyki – zgodnie z zarządzeniem nr 6 Ministra Cyfryzacji z dnia 31 grudnia 2015 r. w sprawie nadania statutu instytucji gospodarki budżetowej pod nazwą „Centralny Ośrodek Informatyki"[2] jest to instytucja gospodarki budżetowej podległa Ministrowi Cyfryzacji (uprzednio Ministrowi Spraw Wewnętrznych);
incydent	zdarzenie, które powoduje lub może spowodować przerwę w dostarczaniu usługi informatycznej lub obniżenie jej jakości;
KN	Komponent Niejawny, jeden z modułów SRP;
MC	Ministerstwo Cyfryzacji;
MSW	Ministerstwo Spraw Wewnętrznych;
MSWiA	Ministerstwo Spraw Wewnętrznych i Administracji;
PESEL	Powszechny Elektroniczny System Ewidencji Ludności, jeden z rejestrów wchodzących w skład SRP;
ePUAP	Elektroniczna Platforma Usług Administracji Publicznej – system teleinformatyczny udostępniający usługi elektroniczne administracji publicznej dla obywateli;
migracja danych	czynność polegająca na przeniesieniu danych z papierowych ksiąg stanu cywilnego (prowadzonych przed 1 marca 2015 r.) i wprowadzeniu tych danych do elektronicznej Bazy Usług Stanu Cywilnego wchodzącego w skład Systemu Rejestrów Państwowych; jako migrację danych należy rozumieć także przeniesienie danych zgromadzonych w systemach informatycznych urzędów miast/miast i gmin/gmin wykorzystywanych przed 1 marca 2015 r. do Systemu Rejestrów Państwowych;
p.a.s.c.	ustawa z dnia 28 listopada 2014 r. – Prawo o aktach stanu cywilnego;
polityka bezpieczeństwa informacji	zbiór reguł i procedur określających organizację i zarządzanie bezpieczeństwem informacji w jednostce;

[1] Źródło: art. 2 ust. 3 ustawy z dnia 28 listopada 2014 r. Prawo o aktach stanu cywilnego (Dz. U. z 2016 r. poz. 2064).

[2] Dz. Urz. MC poz. 7, ze zm.

program *pl.ID* zbiór wspólnie zarządzanych i koordynowanych projektów, których celem jest budowa rozwiązań technicznych mających poprawić jakość usług publicznych świadczonych przez państwo dla obywateli. Program *pl.ID* był objęty dofinansowaniem z Unii Europejskiej w ramach *Programu Operacyjnego Innowacyjna Gospodarka 2007–2013*, 7. Priorytet – *Społeczeństwo informacyjne – budowa elektronicznej administracji*, działanie 7.1 *Społeczeństwo informacyjne – budowa elektronicznej administracji*;

RDO Rejestr Dowodów Osobistych, jeden z rejestrów wchodzących w skład SRP;

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];

sieć OST 112 ogólnopolska sieć teleinformatyczna zapewniająca połączenie między infrastrukturą SRP zlokalizowaną w gminach a centralnym modułem SRP;

SOP System Odznaczeń Państwowych;

SRP System Rejestrów Państwowych – to system informatyczny, za pomocą którego następuje dostęp do głównych rejestrów (ewidencji) państwa, m.in. wykorzystywany przy załatwianiu przez obywateli spraw dotyczących dowodów osobistych, meldunków oraz aktów stanu cywilnego. System Rejestrów Państwowych został wytworzony i uruchomiony na zlecenie MSW, od 2016 r. funkcjonowanie systemu nadzoruje Minister Cyfryzacji;

u.d.o. ustawa z dnia 6 sierpnia 2010 r. o dowodach osobistych[4];

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

umowa SLA (ang. Service Level Agreement) umowa dotycząca poziomu usług informatycznych i ich parametrów;

USC Urząd Stanu Cywilnego – jednostka organizacyjna wchodząca w skład urzędu gminy. Kierownikiem urzędu stanu cywilnego jest wójt (burmistrz, prezydent miasta);

ustawa o informatyzacji ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne[5];

ustawa o NIK ustawa z dnia 23 grudnia 1994 r. o Najwyższej Izbie Kontroli[6];

walidacja danych sprawdzenie poprawności danych wprowadzanych do systemu;

właściciel SRP do 31 grudnia 2015 r. minister właściwy do spraw wewnętrznych, od 1 stycznia 2016 r. minister właściwy do spraw informatyzacji.

---

3 Dz. U. z 2016 r. poz. 113, ze zm.

4 Dz. U. z 2016 r. poz. 391, ze zm.

5 Dz. U. z 2014 r. poz. 1114, ze zm.

6 Dz. U. z 2015 r. poz. 1096, ze zm.

1 ZAŁOŻENIA KONTROLI

Temat i numer kontroli

System Rejestrów Państwowych – bezpieczeństwo, funkcjonowanie i użyteczność (P/16/006)

Uzasadnienie podjęcia kontroli

Kontrola została podjęta z inicjatywy własnej NIK. Z dniem 1 marca 2015 r. zastąpiono, używane dotychczas w niektórych urzędach miast/miast i gmin/gmin systemy informatyczne, jednolitym w skali kraju Systemem Rejestrów Państwowych. System ten tworzą m.in. trzy najbardziej istotne dla obywateli i państwa rejestry, tj. Rejestr PESEL, Rejestr Dowodów Osobistych oraz Rejestr Stanu Cywilnego. Udostępnienie SRP umożliwiło załatwianie przez obywateli spraw dotyczących dowodów osobistych lub aktów stanu cywilnego w dowolnym urzędzie gminy, niezależnie od miejsca zamieszkania. Z informacji prasowych wynikało, że wraz z uruchomieniem SRP i udostępnieniem go jednostkom samorządu terytorialnego, użytkownicy sygnalizowali występowanie wielu błędów i braków w aplikacji „Źródło", a w urzędach stanu cywilnego w wielu miastach Polski zaczęły powstawać opóźnienia w obsłudze obywateli.

Wprowadzenie

Integracja rejestrów państwowych w SRP była jednym z celów programu *pl.ID – polska ID karta*. W latach 2009–2012 za jego realizację było odpowiedzialne Centrum Projektów Informatycznych. W 2012 r., w związku ze zidentyfikowaniem istotnych problemów dotyczących założeń, przyjętej sekwencji prac i możliwości osiągnięcia zakładanych rezultatów, zmodyfikowano zakres przedsięwzięcia skupiając prace na stworzeniu jednolitego i spójnego Systemu Rejestrów Państwowych. Od 2013 r. przygotowanie i wdrożenie Systemu Rejestrów Państwowych było realizowane w ramach zarządzanego przez Ministra Spraw Wewnętrznych programu *pl.ID*. W umowie nr 4/DSiA/2013 z 25 lutego 2013 r. Minister Spraw Wewnętrznych powierzył zadania z tego zakresu Centralnemu Ośrodkowi Informatyki.

Z dniem 16 listopada 2015 r. MSW zostało przekształcone w MSWiA[7] i nadzór nad COI objął Minister Spraw Wewnętrznych i Administracji. Od 1 stycznia 2016 r. funkcję organu nadzorującego COI przejął Minister Cyfryzacji[8].

Cel i zakres kontroli

Celem kontroli była ocena Systemu Rejestrów Państwowych pod kątem zapewnienia bezpieczeństwa danych, funkcjonalności oraz poprawy obsługi obywateli. W związku z tym ocenie poddano następujące, wybrane kwestie:

- realizację przez Centralny Ośrodek Informatyki zadań związanych z wykonaniem, utrzymaniem i rozwojem Systemu Rejestrów Państwowych;
- realizację przez urzędy miast/miast i gmin zadań z wykorzystaniem Systemu Rejestrów Państwowych, w szczególności:
  - wsparcie przez SRP procesu obsługi obywatela – funkcjonalność i efektywność aplikacji „Źródło";

[7] Na podstawie rozporządzenia Rady Ministrów z dnia 20 listopada 2015 r. w sprawie utworzenia Ministerstwa Spraw Wewnętrznych i Administracji (Dz. U. poz. 1946), które weszło w życie z dniem 24 listopada 2015 r., z mocą od 16 listopada 2015 r.

[8] Na podstawie art. 42 ustawy z dnia 22 grudnia 2015 r. o zmianie ustawy o działach administracji rządowej oraz niektórych innych ustaw (Dz. U. poz. 2281, ze zm.).

- wpływ wdrażania wymaganych funkcjonalności i elementów SRP oraz zasilania tego systemu danymi na sprawność pracy użytkowników w urzędach miast/miast i gmin;
- zapewnienie bezpieczeństwa SRP i jego danych;
- wpływ uruchomienia SRP na funkcjonowanie wewnętrznych systemów informatycznych urzędów miast/miast i gmin wykorzystywanych do realizacji pozostałych spraw z zakresu obsługi obywatela;
- wpływ udostępnienia SRP na koszty obsługi zadań w urzędach miast/miast i gmin;
- wpływ uruchomienia SRP na ograniczenie rozbieżności pomiędzy danymi zawartymi w poszczególnych rejestrach wchodzących w skład tego systemu.

Kontrolą objęto 14 jednostek, tj. Centralny Ośrodek Informatyki oraz 13 jednostek samorządu terytorialnego z terenu województw: dolnośląskiego, mazowieckiego, podkarpackiego i podlaskiego. Wykaz jednostek, w których przeprowadzono kontrolę zawiera załącznik nr 2 do Informacji.

W trakcie kontroli, na podstawie art. 29 ust. 1 pkt 2 lit. f ustawy o NIK, uzyskano dodatkowe informacje z Ministerstwa Cyfryzacji oraz Ministerstwa Spraw Wewnętrznych i Administracji.

Wyboru jednostek do kontroli dokonano w sposób celowy, wybierając większe urzędy miast/miast i gmin liczących co najmniej 40 tys. mieszkańców. Wynikało to z założenia, że na skutek odmiejscowienia załatwiania spraw, wielu obywateli korzysta z możliwości załatwienia sprawy w miejscu aktualnego zamieszkania lub zatrudnienia. W większości przypadków są to większe ośrodki miejskie.

Kontrolę w COI przeprowadzono na podstawie art. 2 ust. 1 ustawy o NIK, z uwzględnieniem kryteriów określonych w art. 5 ust. 1 ww. ustawy, tj. pod względem legalności, gospodarności, rzetelności i celowości. W jednostkach samorządu terytorialnego kontrolę przeprowadzono na podstawie art. 2 ust. 2 w związku z art. 5 ust. 2 ustawy o NIK, tj. pod względem legalności, rzetelności i gospodarności.

Kontrolą objęto okres od 1 stycznia 2013 r. do 31 lipca 2016 r.

Czynności kontrolne przeprowadzono w okresie od 1 czerwca do 28 października 2016 r.

2 PODSUMOWANIE WYNIKÓW KONTROLI

2.1 Ocena kontrolowanej działalności

Przygotowanie i udostępnienie Systemu Rejestrów Państwowych w ramach programu *pl.ID* obarczone było wieloma błędami, co spowodowało, że w trakcie użytkowania systemu wystąpiły utrudnienia dla obywateli oraz urzędów korzystających z SRP. System uruchomiono z dwumiesięcznym opóźnieniem, a po jego udostępnieniu ujawniło się wiele usterek (problemów), a także braki w funkcjonalnościach w aplikacji „Źródło" wykorzystywanej w urzędach do obsługi spraw obywateli. Opóźnienia wynikały z przyczyn leżących zarówno po stronie zlecającego budowę SRP (Ministerstwo Spraw Wewnętrznych), jak i wykonawcy (Centralny Ośrodek Informatyki). Minister Cyfryzacji oraz COI podjęli działania w celu wyeliminowania stwierdzonych błędów i wprowadzenia oczekiwanych przez użytkowników funkcjonalności. Ponadto, wprowadzenie SRP ujawniło szereg niezgodności w danych o obywatelach zgromadzonych w poszczególnych rejestrach wchodzących w skład SRP. Kontrolowane urzędy miast podejmowały działania w celu korygowania ujawnianych niezgodności.

Istotne jest, że wraz z udostępnieniem SRP nastąpiło odmiejscowienie załatwiania spraw dotyczących dowodów osobistych oraz wydawania odpisów aktów stanu cywilnego, dzięki czemu obywatele mogą załatwiać te sprawy w dowolnym urzędzie (niezależnie od miejsca zamieszkania). Nieuwzględnienie przez MSW, na etapie przygotowywania programu *pl.ID*, masowej migracji aktów stanu cywilnego do SRP z lokalnych systemów informatycznych wpłynęło na opóźnienia w wydawaniu odpisów aktów stanu cywilnego, szczególnie w dużych ośrodkach miejskich.

Zarządzanie bezpieczeństwem SRP nie zostało kompleksowo zorganizowane i uregulowane. MSW wprowadziło wprawdzie w 2015 r. politykę bezpieczeństwa SRP, jednak w zasadniczej części miała ona charakter deklaratywny, gdyż nie zawierała szczegółowych rozwiązań umożliwiających sprawne i skuteczne zarządzanie bezpieczeństwem SRP[9]. W ośmiu urzędach miast (62% badanych) nie opracowano i nie wdrożono polityk bezpieczeństwa informacji, a w trzech (23% badanych) nie przestrzegano wymogu zablokowania dostępu do Internetu na komputerach wykorzystywanych do pracy z SRP. Opracowanie i wdrożenie ww. rozwiązań z zakresu bezpieczeństwa ma szczególne znaczenie dla zapewnienia bezpieczeństwa danych o obywatelach.

Ocenę powyższą uzasadniają następujące ustalenia kontroli:

- COI wywiązał się z powierzonych mu zadań w zakresie budowy SRP, system został udostępniony z dniem 1 marca 2015 r., jednak nastąpiło to z opóźnieniem w stosunku do pierwotnej daty 1 stycznia 2015 r.[10], zaś w SRP istniało wiele błędów rzutujących na sprawność pracy użytkowników końcowych w systemie. Utrudniło to sprawną realizację zadań przez użytkowników SRP. Opóźnienie w uruchomieniu SRP i błędy w jego działaniu wynikały w szczególności z:

9 Na dzień zakończenia kontroli w COI (8 września 2016 r.) rozwiązania takie nie zostały jeszcze opracowane i wdrożone przez Ministra Cyfryzacji, który od 1 stycznia 2016 r. odpowiada za SRP.

10 Termin udostępnienia SRP w dniu 1 stycznia 2015 r. wynikał z pierwotnego tekstu ustawy Prawo o aktach stanu cywilnego oraz ustawy z dnia 7 grudnia 2012 r. o zmianie ustawy o ewidencji ludności i o dowodach osobistych oraz niektórych innych ustaw (Dz. U. poz. 1407). Ustawą z dnia 19 grudnia 2014 r. o zmianie ustawy o dowodach osobistych, ustawy o ewidencji ludności oraz ustawy – Prawo o aktach stanu cywilnego (Dz. U. poz. 1888), termin udostępnienia SRP został przesunięty na 1 marca 2015 r.

  - braku skutecznego, konsekwentnego stosowania metodyk zarządzania projektami (m.in. przedstawiciele MSW nie brali udziału w części spotkań w COI dotyczących wytwarzania oprogramowania SRP przy zastosowaniu metodyki *Scrum*[11]); [str. 16–17]
  - błędów w oprogramowaniu opracowanym przez COI, w związku z czym SRP został odebrany i uruchomiony warunkowo po upływie dwóch miesięcy od pierwotnie planowanego terminu; [str. 17–18]
  - zgłaszania przez użytkowników dodatkowych wymagań co do funkcjonalności SRP w trakcie testów oprogramowania; [str. 18]
  - zbyt krótkiego czasu na realizację projektu, co niekorzystnie wpłynęło na jakość udostępnionego systemu; [str. 17–21]
  - równolegle prowadzonych prac nad aktami prawnymi z zakresu rejestracji stanu cywilnego i prac programistycznych przy budowie SRP; [str. 18]
  - braku decyzji MSW o przeprowadzeniu przez COI wdrożenia pilotażowego, które pozwoliłoby na przetestowanie systemu w praktyce oraz wykrycie i usunięcie wad. [str. 19]
- MSW nie przewidziało w ramach programu *pl.ID* masowej migracji aktów stanu cywilnego do BUSC w SRP, zgromadzonych w postaci elektronicznej w lokalnych systemach informatycznych urzędów gmin wykorzystywanych przed 1 marca 2015 r., w związku z czym po uruchomieniu SRP występowały opóźnienia w wydawaniu obywatelom odpisów aktów stanu cywilnego. [str. 24–26]
- W sześciu kontrolowanych urzędach[12] wystąpiły opóźnienia w realizacji części zleceń migracji gdyż wprowadzanie do aplikacji „Źródło" danych w zakresie aktów stanu cywilnego następowało po 10 dniach od dnia otrzymania zlecenia z innego urzędu, co stanowiło naruszenie art. 125 ust. 4 p.a.s.c. Uniemożliwiało to wydanie obywatelowi odpisu aktu stanu cywilnego w terminie 10 dni od dnia złożenia przez niego wniosku. Uruchomienie SRP umożliwiło obywatelom załatwianie spraw w zakresie wydawania odpisów aktów stanu cywilnego oraz dowodów osobistych w dowolnym USC, bądź urzędzie gminy (tzw. odmiejscowienie). [str. 26–27]
- Opracowane i stosowane przez COI procedury eksploatacyjne i awaryjne pozwalały na zapewnienie ciągłości działania SRP. [str. 28]
- Raporty za okres od czerwca 2015 r. do lipca 2016 r. wskazywały, że dostępność SRP kształtowała się na poziomie od 99,93% do 100%, przy czym osiągnięta dostępność SRP nie oznacza, że działanie systemu było wolne od usterek/błędów, tylko że jego funkcje lub usługi były dostępne. Ponadto, analiza incydentów zgłoszonych w okresie od 1 marca 2015 r. do 15 czerwca 2016 r. wykazała, iż miesięczne raporty z wykonania usług SRP sporządzane w COI nie uwzględniały niektórych incydentów. [str. 29–30]
- Ustalone w umowie na utrzymanie SRP okresy rozwiązywania i usuwania przez COI problemów związanych z funkcjonowaniem tego systemu są zbyt długie. Przewidziany umową maksymalny czas na usunięcie incydentu krytycznego wynosi trzy dni robocze. [str. 27–28]
- Wsparcie techniczne dla użytkowników SRP zostało zorganizowane w COI zgodnie ze współczesną praktyką w tym zakresie, jednak czas oczekiwania na rozwiązanie części zgłoszeń o problemach w działaniu SRP, był zbyt długi i w skrajnych przypadkach sięgał ponad roku. [str. 31–33]

[11] *Scrum* – metodyka prowadzenia projektów, która zakłada podział prac na mniejsze etapy i umożliwia elastyczne reagowanie na uwagi uczestników projektu.

[12] UM: Łomża, Piaseczno, Przemyśl, Wałbrzych, Warszawa, Wrocław.

- Stosowane przez COI mechanizmy wdrażania zmian w oprogramowaniu SRP były właściwe, bowiem pozwalały na zminimalizowanie negatywnego wpływu wprowadzania tych zmian na usługi już funkcjonujące w środowisku produkcyjnym. [str. 33]
- COI podjął działania zmierzające do zapewnienia rozwoju SRP, występując do MSW z propozycją przeznaczenia części zysku COI na działania rozwojowe oraz opracowując projekt ramowej umowy rozwojowej. Zawarcie umowy dotyczącej rozwoju dopiero 29 czerwca 2016 r. było opóźnione w stosunku do skali zidentyfikowanych potrzeb rozwojowych oraz utrudniło wprowadzanie nowych, a także rozbudowę istniejących funkcjonalności SRP. [str. 15–16]
- COI podejmował działania w celu zapewnienia bezpieczeństwa SRP w zakresie mu powierzonym. [str. 35]
- MSW wprowadziło w 2015 r. politykę bezpieczeństwa SRP, jednak nie określiło zasad funkcjonowania Systemu Zarządzania Bezpieczeństwem Informacji. Na dzień zakończenia kontroli zasady te nie zostały opisane i wdrożone przez właściciela SRP (Ministra Cyfryzacji). [str. 35–36]
- W ośmiu kontrolowanych urzędach[13] (tj. 62%) nie opracowano i nie wdrożono polityki bezpieczeństwa informacji, która jest elementem systemu zarządzania bezpieczeństwem informacji, wymaganym przez przepis § 20 ust. 3 w związku z ust. 1 rozporządzenia KRI. [str. 38]
- W pięciu kontrolowanych urzędach[14] (tj. 38%) wystąpiły nieprawidłowości w zakresie blokowania lub odbierania dostępu do aplikacji „Źródło" byłym pracownikom. [str. 39–40]
- W trzech urzędach[15] (tj. 23%) stacje komputerowe[16] z aplikacją „Źródło" posiadały dostęp do Internetu. Było to niezgodne z *Wymaganiami dla stacji roboczych stanowisk obsługi dla użytkowników końcowych SRP*[17]. [str. 41]
- W trzech urzędach (tj. 23%) w okresie objętym kontrolą nie przeprowadzano audytu w zakresie bezpieczeństwa informacji w systemach informatycznych, co było niezgodne z przepisem § 20 ust. 2 pkt 14 rozporządzenia KRI. [str. 42]
- W dziewięciu kontrolowanych urzędach miast (tj. 69%) po wdrożeniu SRP nastąpił wzrost kosztów załatwiania spraw, gdyż zaistniała konieczność zatrudnienia dodatkowych pracowników oraz zlecania dodatkowych prac w ramach godzin nadliczbowych lub umów cywilnoprawnych. Przyczyną tego było nieprzeprowadzenie masowej migracji aktów stanu cywilnego zgromadzonych w lokalnych systemach informatycznych oraz zwiększona liczba interesantów w urzędach dużych miast w związku z odmiejscowieniem załatwiania spraw dotyczących dowodów osobistych oraz wydawania odpisów aktów stanu cywilnego. [str. 43–44]
- We wszystkich kontrolowanych urzędach identyfikowano rozbieżności pomiędzy danymi zgromadzonymi w poszczególnych rejestrach wchodzących w skład SRP (PESEL, RDO, BUSC) oraz pomiędzy danymi zawartymi we wnioskach a tymi rejestrami. W urzędach podejmowano działania mające na celu wyjaśnienie i skorygowanie ujawnionych rozbieżności. [str. 46]

13 Dotyczy UM: Bielsk Podlaski, Krosno, Legionowo, Łomża, Piaseczno, Przemyśl, Rzeszów, Warszawa.
14 UM: Przemyśl, Łomża, Bielsk Podlaski, Świdnica, Wrocław.
15 UM: Warszawa, Łomża, Otwock.
16 Komputer wykorzystywany do bezpośredniej pracy z aplikacją „Źródło".
17 Wydane przez Ministerstwo Spraw Wewnętrznych i Centralny Ośrodek Informatyki.

2.2 Uwagi i wnioski

1. NIK zwraca uwagę na problemy w zarządzaniu programem *pl.ID*, w ramach którego wytworzono i udostępniono SRP. W szczególności problemy te dotyczyły: częstych zmian na stanowisku kierownika programu, prowadzenia przez MSW harmonogramu projektów bez korzystania z narzędzi kontroli postępu prac, rezygnacji przedstawicieli MSW z udziału w spotkaniach mających na celu bieżącą ocenę funkcjonalności w wytwarzanym oprogramowaniu SRP, jak również nieprzeprowadzenia pilotażowego wdrożenia systemu. Według NIK, prowadząc tak złożone projekty informatyczne należy konsekwentnie stosować uznane metody zarządzania projektami oraz należy uwzględniać dobre praktyki w tym zakresie, co może wpłynąć na sprawniejsze zarządzanie projektem i poprawić jakość wytwarzanego produktu.
2. Należy kontynuować działania COI (we współpracy z MC) mające na celu wyeliminowanie błędów w działaniu systemu, a także wprowadzenie rozwiązań poprawiających działanie poszczególnych funkcjonalności wykorzystywanych przez użytkowników końcowych SRP. Aktywne włączenie w te prace użytkowników końcowych (urzędów miast) może wpłynąć na wyeliminowanie szeregu błędów w działaniu systemu, a także ułatwić rozwój SRP. Użytkownicy aplikacji „Źródło" zwracali uwagę na potrzebę ułatwienia obsługi załatwiania spraw z wykorzystaniem tej aplikacji, gdyż np. wydanie kilku odpisów tego samego aktu stanu cywilnego wymagało wielokrotnego wykonania tych samych czynności w aplikacji.
3. Ustalone w umowie na utrzymanie SRP okresy rozwiązywania i usuwania incydentów (problemów) związanych z funkcjonowaniem SRP są zbyt długie, gdyż zgodnie z umową pomiędzy MC i COI w przypadku wystąpienia w funkcjonowaniu SRP incydentu krytycznego, usuwanie awarii może trwać nawet trzy dni, co oznacza trzydniową przerwę w działaniu systemu, a w konsekwencji brak możliwości bieżącej rejestracji narodzin, małżeństw czy zgonów.
4. Brak przeprowadzenia masowej migracji aktów stanu cywilnego do SRP, błędy w organizacji zapewnienia bezpieczeństwa SRP, a także zawarcie umowy dotyczącej rozwoju SRP dopiero po ponad roku od jego udostepnienia wskazują na niewłaściwe zarządzanie ryzykami w obszarach bezpieczeństwa, funkcjonalności i użyteczności na etapie przygotowania systemu i w trakcie pierwszego roku funkcjonowania SRP.
5. Masowa migracja danych z zakresu aktów stanu cywilnego do modułu BUSC w SRP, przy wykorzystaniu narzędzia opracowywanego przez COI, może się w istotny sposób przyczynić do zapewnienia sprawniejszego załatwiania spraw obywateli przez USC. Przeprowadzenie powyższej migracji umożliwiłoby bowiem wykorzystanie danych elektronicznych zgromadzonych już w lokalnych systemach informatycznych (wykorzystywanych do obsługi aktów stanu cywilnego przed uruchomieniem SRP) bez konieczności ich każdorazowego, pojedynczego wprowadzania do SRP, co mogłoby znacznie przyspieszyć obsługę obywateli.
6. Stwierdzone w trakcie kontroli NIK opóźnienia w wydawaniu obywatelom odpisów aktów stanu cywilnego, szczególnie w dużych ośrodkach miejskich, mogą ulec zmniejszeniu w związku z wprowadzoną przez Sejm, z inicjatywy MC, nowelizacją ustawy p.a.s.c.[18], która weszła w życie z dniem 27 sierpnia 2016 r. Zmiany w przepisach umożliwiają m.in. sprawniejsze przenoszenie do rejestru stanu cywilnego aktów sporządzonych w papierowych księgach, dzięki uprawnieniu

[18] Ustawa z dnia 6 lipca 2016 r. o zmianie ustawy Prawo o aktach stanu cywilnego (Dz. U. poz. 1221).

kierownika USC do upoważnienia pracowników do dokonania tej czynności. Zmiany te umożliwiły również tymczasowe wydawanie przez pięć lat odpisów aktów stanu cywilnego na podstawie danych z lokalnych aplikacji wykorzystywanych w USC przed 1 marca 2015 r.

7. Dla zapewnienia prawidłowej i bezpiecznej realizacji spraw z wykorzystaniem danych o obywatelach, zgromadzonych w systemach informatycznych wykorzystywanych przez urzędy miast, istotnym jest zapewnienie bezpieczeństwa tych danych. Służyć temu powinien prawidłowo funkcjonujący system zarządzania bezpieczeństwem informacji, w szczególności przyjęcie i konsekwentne wdrożenie oraz stosowanie polityki bezpieczeństwa informacji. Tymczasem kontrola NIK wykazała, że w tym obszarze wystąpiło wiele nieprawidłowości w urzędach polegających na niedochowaniu wymogów określonych w § 20 rozporządzenia KRI, w szczególności na braku opracowania i wdrożenia polityki bezpieczeństwa informacji oraz nieprzeprowadzaniu audytu w zakresie bezpieczeństwa informacji.

8. Szczególnie istotny dla zapewnienia bezpieczeństwa przetwarzania informacji w SRP jest wprowadzony przez COI wymóg zablokowania dostępu do Internetu na stacjach komputerowych z aplikacją „Źródło". Dokument COI *Wymagania dla stacji roboczych* nie przewiduje wyjątków ani odstępstw od tej reguły, wytyczne wydane przez COI dotyczą wszystkich urzędów realizujących zadania w SRP z wykorzystaniem aplikacji „Źródło". Należy przy tym wskazać, że dotychczas MC oraz MSWiA nie wypracowały i nie wdrożyły skutecznych rozwiązań w zakresie egzekwowania od kierowników urzędów wymogu odłączenia od Internetu stacji komputerowych z aplikacją „Źródło".

9. Audyty i testy bezpieczeństwa SRP przeprowadzane były jedynie w trakcie jego wytwarzania i wdrażania, natomiast przez prawie półtora roku od chwili jego uruchomienia, pomimo wprowadzenia licznych zmian w tym systemie, nie przeprowadzono żadnego audytu/testu bezpieczeństwa.

10. Zdaniem NIK, trudność zorganizowania zapewnienia bezpieczeństwa SRP jako całości wynika z rozproszenia infrastruktury systemu pomiędzy wieloma podmiotami, m.in.: MC, COI, administrację rządową i samorządową, przy czym obowiązki każdej ze stron nie są w tym zakresie jednoznacznie określone. Organizacja zarządzania bezpieczeństwem SRP powinna być w głównej mierze ustanowiona przez właściciela systemu, czyli Ministra Cyfryzacji. Obowiązująca *Polityka Bezpieczeństwa pl.ID*, opracowana jeszcze przez MSW, nie zawiera szczegółowych procedur umożliwiających sprawne zarządzanie bezpieczeństwem informacji SRP. Dotychczasowy sposób zarządzania bezpieczeństwem informacji skutkuje tym, że kwestie bezpieczeństwa SRP nie są traktowane w sposób systematyczny, w ramach jasno zdefiniowanego, jednolitego podejścia zgodnego z dobrą, ustandaryzowaną praktyką zawartą w normie ISO 27001[19].

***

Do burmistrzów i prezydentów miast zostały skierowane wnioski dotyczące usunięcia stwierdzonych w trakcie kontroli nieprawidłowości. Dotyczyły one głównie:

- zapewnienia terminowego dokonywania migracji aktów stanu cywilnego na wnioski z innych urzędów do rejestru stanu cywilnego;
- opracowania i wdrożenia polityki bezpieczeństwa informacji;

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

- uniemożliwienia w sposób trwały dostępu do Internetu na stacjach komputerowych, na których wykorzystywana jest aplikacja „Źródło";
- niezwłocznego odbierania uprawnień użytkownikom aplikacji „Źródło" w chwili zakończenia zatrudnienia lub zmiany zakresu obowiązków;
- przeprowadzania corocznych audytów z zakresu bezpieczeństwa informacji.

W związku z ustaleniami kontroli, Najwyższa Izba Kontroli wnioskuje do Ministra Cyfryzacji o:

- przeprowadzenie masowej migracji do rejestru BUSC danych zgromadzonych w lokalnych systemach informatycznych, co powinno wpłynąć na poprawę terminowości wydawania odpisów aktów stanu cywilnego;
- opracowanie szczegółowych procedur w ramach *Polityki bezpieczeństwa pl.ID*;
- wypracowanie rozwiązań umożliwiających egzekwowanie od kierowników urzędów wymogu odseparowania stacji komputerowych z aplikacją „Źródło" od sieci Internet;
- zapewnienie usunięcia przez COI pozostających jeszcze błędów w oprogramowaniu oraz poprawy funkcjonalności SRP pod kątem wymagań użytkowników końcowych;
- podjęcie działań w celu zagwarantowania krótszych okresów usuwania awarii SRP, określonych w obowiązującej umowie z COI na utrzymanie tego systemu.

3 WAŻNIEJSZE WYNIKI KONTROLI

3.1 Wsparcie procesu obsługi obywatela i wpływ SRP na optymalizację procesów administracyjnych. Funkcjonalność i efektywność aplikacji „Źródło"

Wydatki na przygotowanie, uruchomienie i udostępnienie SRP

1. System Rejestrów Państwowych był przygotowywany przez COI w latach 2013–2015, w oparciu o kolejne zlecenia Ministra Spraw Wewnętrznych, udzielane na podstawie ramowej umowy nr 4/DSiA/2013. COI realizował w szczególności zadania: budowy nowych i modernizacji istniejących rejestrów państwowych, optymalizacji aplikacji dostępowej, budowy komponentu niejawnego Systemu Rejestrów Państwowych, modernizacji serwerowni, dostarczenia i instalacji infrastruktury informatycznej dla dwóch ośrodków przetwarzania danych oraz na potrzeby funkcjonującego w ramach SRP komponentu niejawnego.

Maksymalne wynagrodzenie COI z tytułu realizacji umowy nr 4/DSiA/2013 ustalono w wysokości 121 623,5 tys. zł. Kwota ta, na podstawie aneksu do ww. umowy[20], wyniosła 109 000,0 tys. zł.

2. Do 2012 r., na mocy porozumień zawartych pomiędzy Ministrem Spraw Wewnętrznych i Administracji a jednostkami samorządu terytorialnego, gminy zostały wyposażone w sprzęt komputerowy i aplikacje teleinformatyczne, w celu obsługi spraw z zakresu dowodów osobistych, aktów stanu cywilnego oraz ewidencji ludności. Łącznie użyczono 43,1 tys. sztuk sprzętu informatycznego[21]. Ponadto, w 2015 r. na podstawie przeprowadzonych przez MSW ankiet dotyczących inwentaryzacji użyczonego sprzętu i identyfikacji potrzeb w zakresie doposażenia, 1 763 gminom przekazano dodatkowo 6,7 tys. sztuk zestawów komputerowych, drukarek i skanerów. Użyczony sprzęt zgodnie z treścią porozumień powinien być wykorzystywany do obsługi spraw z zakresu ewidencji ludności oraz wydawania dowodów osobistych i aktów stanu cywilnego. Minister Cyfryzacji poinformowała, że nie zostały określone zasady postępowania z użyczonym sprzętem po okresie trwałości dla projektu dofinansowanego ze środków UE, upływającym z końcem 2024 r.

3. Według danych Ministerstwa Cyfryzacji za wydatki niekwalifikowalne w ramach programu *pl.ID* w latach 2013–2015 uznano łącznie 31 274,4 tys. zł. Wydatki te dotyczyły zrealizowanych, na podstawie zleceń[22] MSW, prac własnych COI, tj. prac programistycznych i projektów technicznych. Ze względu na brak możliwości udokumentowania tych wydatków w zakresie wynikającym z zasad kwalifikowalności[23] zostały one wyłączone z procesu certyfikacji do Komisji Europejskiej. Minister Cyfryzacji poinformowała, że zgodnie z decyzją podjętą w MC już po przejęciu programu *pl.ID*, wyłączeniu z wniosków o płatność będzie podlegać również część wydatków poniesiona przez Centrum Projektów Informatycznych na wytworzenie oprogramowania w zakresie, w którym oprogramowanie to nie zostało wykorzystane w programie *pl.ID*. Na dzień zakończenia czynności kontrolnych kwota tych wydatków wynosiła 38 808,3 tys. zł.

---

20 Aneks nr 3 do umowy nr 4/DSiA/2013 z 28 lutego 2015 r.

21 W tym m.in.: zestawy komputerowe, serwery, czytniki kart, drukarki, routery.

22 W ramach umowy nr 4/DSiA/2013.

23 *Krajowe wytyczne dotyczące kwalifikowania wydatków w ramach funduszy strukturalnych i Funduszu Spójności w okresie programowania 2007–2013*, opublikowane na stronie: https://www.funduszeeuropejskie.2007–2013.gov.pl/Dokumenty/wytycznepolskie/Strony/glowna.aspx

Wydatki na utrzymanie SRP

W latach 2015 i 2016 r. zadania w zakresie utrzymania SRP realizowane były przez COI na podstawie pięciu umów zawartych z MSW, MSWiA i MC[24]. Zakres umów obejmował świadczenie usług zapewniających poprawne i nieprzerwane funkcjonowanie SRP, tj.:

- utrzymanie właściwego poziomu jakościowego usług dla użytkowników m.in.: poprzez zarządzanie incydentami (w tym prowadzenie Service Desk), problemami, zmianą, poziomem usług, konfiguracją, dostępnością i pojemnością (zasobami), bezpieczeństwem, ciągłością działania, wiedzą, a także serwis oprogramowania, komunikację i szkolenia;
- świadczenie usług dodatkowych, m.in.: modyfikacje, zmiany oprogramowania, rozwój aplikacji wspomagających eksploatację, utrzymanie i zarządzanie systemem, prowadzenie działań konsultacyjnych, eksperckich i analitycznych.

Wynagrodzenie COI z tytułu utrzymania SRP w okresie od 1 marca 2015 r. do 30 czerwca 2019 r. określono w łącznej wysokości 96 933,9 tys. zł. Według stanu na 31 maja 2016 r. na utrzymanie SRP wydatkowano łącznie 20 399,7 tys. zł. Kwota ta stanowiła 21% kwoty zaplanowanej na realizację zadań w zakresie utrzymania SRP.

Wydatki na rozwój SRP

W ustawie budżetowej na 2015 r. MSW nie zaplanowało środków na rozwój SRP przez COI. W ramach prac nad ustawą budżetową na 2016 r. MSW wnioskowało o zabezpieczenie środków na ten cel, jednak ostatecznie nie zostały one przyznane. Jak wyjaśnił Dyrektor COI, począwszy od 2014 r. przedstawiciele COI sygnalizowali MSW potrzebę rozwoju i modernizacji SRP. W związku z powyższym COI m.in. wystąpił do Ministra Spraw Wewnętrznych z propozycją podziału wypracowanego zysku COI i przeznaczenia jego części na rozwój SRP oraz opracował i przekazał do MSW projekt ramowej umowy rozwojowej. Ministerstwo Spraw Wewnętrznych podjęło działania w celu oceny możliwości podziału zysku według propozycji COI, jednak ostatecznie środki te zwiększyły fundusz COI.

W dniu 29 czerwca 2016 r. w wyniku uzgodnień pomiędzy MC i COI, została zawarta umowa na rozwój SRP na okres czterech lat, na łączną kwotę nie przekraczającą 27 293,3 tys. zł.

Zawarcie umowy na rozwój dopiero po ponad roku od udostępnienia SRP uniemożliwiło bieżące wprowadzanie zmian w wytworzonym oprogramowaniu SRP. Zawarcie tej umowy miało zasadnicze znaczenie dla umożliwienia COI prowadzenia prac rozwojowych SRP, w tym dla zapewnienia dostosowywania funkcjonalności SRP do zmian w przepisach prawnych oraz wprowadzenia do systemu zmian zgłaszanych przez użytkowników końcowych SRP.

W trakcie prac nad ustawą budżetową na 2017 r. MC zgłosiło do ujęcia w części 83 – *Rezerwy celowe* kwotę w wysokości 78 000,0 tys. zł na utrzymanie i rozwój SRP i Zintegrowanej Infrastruktury Rejestrów[25].

[24] Umowy: 1/U/COI/MSW/2015 z 28 lutego 2015 r., zawarta pomiędzy MSW i COI, 3/DT/4.13/2015 (5/U/COI/MSW/2015) z 29 maja 2015 r., zawarta pomiędzy MSW i COI, 4/DT/4.13/2015/bp (4/U/COI/MSW/2015) z 29 maja 2015 r., zawarta pomiędzy MSW i COI, 11/DT/4.13/2015 (12/U/COI/MSW/2015) z 22 grudnia 2015 r., zawarta pomiędzy MSWiA i COI, 2/DIT/U/COI/2016 z 30 czerwca 2016 r., zawarta pomiędzy MC i COI.

[25] Zintegrowana infrastruktura teleinformatyczna służąca prowadzeniu ewidencji państwowych, w tym SRP.

W związku z koniecznością opracowania Wieloletniego Planu Finansowego Państwa na lata 2016–2019, w materiałach przekazanych do Ministra Finansów zostały zgłoszone do ujęcia w części 27 – *Informatyzacja* środki na centralne systemy ewidencji państwowych, w tym na utrzymanie i rozwój SRP, odpowiednio: 42 663,0 tys. zł na 2018 r. i 43 154,0 tys. zł na 2019 r. Ponadto, zostały zgłoszone do rezerwy celowej środki na m.in. utrzymanie, udostępnianie, eksploatację i rozwój SRP, odpowiednio: 9 483,0 tys. zł na 2018 r. i 9 720 tys. zł na 2019 r.

Zarządzanie programem *pl.ID* w zakresie dotyczącym SRP

Program *pl.ID* był zarządzany przez MSW w oparciu o metodykę MSP[26] oraz metodykę PRINCE2[27]. W ramach realizacji programu wyodrębniono pięć projektów, tj.: *System Rejestrów Państwowych*, *Rejestr Dowodów Osobistych*, *Rejestracja Stanu Cywilnego*, *Legalizacja* i *Serwerownia*. Struktury zarządzania programem i projektami zostały określone formalnie w zarządzeniach Ministra Spraw Wewnętrznych[28].

W związku z realizacją programu *pl.ID* Minister Spraw Wewnętrznych powołał m.in. radę programu, będącą ciałem doradczym, w której mogli uczestniczyć, na zaproszenie przewodniczącego rady, przedstawiciele COI jako wykonawcy SRP. Przedstawiciele COI uczestniczyli w posiedzeniach Rady w charakterze obserwatora i przysługiwał im jedynie głos doradczy, w związku z czym nie mieli oni realnego wpływu na decyzje podejmowane przez radę. W okresie realizacji umowy nr 4/DSiA/2013, tj. od 25 lutego 2013 r. do 31 grudnia 2015 r., odbyło się jedynie sześć posiedzeń rady programu. Za koordynację prac kierowników poszczególnych projektów, koordynację realizacji umowy i współpracę z COI odpowiadał powoływany przez MSW kierownik programu. W trakcie realizacji programu *pl.ID* aż siedmiokrotnie nastąpiła zmiana na tym stanowisku. **Według NIK, częste zmiany na tym stanowisku wpłynęły negatywnie na zapewnienie ciągłości zarządzania programem i współpracę z COI.**

Na poziomie projektów wyodrębnionych w ramach programu *pl.ID* w skład struktur zarządczych wchodzili kierownicy komórek organizacyjnych MSW oraz Centrum Personalizacji Dokumentów[29], kierownicy projektów i zespoły projektowe. W strukturach tych nie zostały utworzone Komitety Sterujące, które zgodnie z metodyką PRINCE2 odpowiadają za ogólne ukierunkowanie i zarządzanie strategiczne projektem. Utrudniło to przepływ informacji pomiędzy wszystkimi interesariuszami, m.in. pomiędzy MSW i COI. Realizując projekty MSW nie stosowało całościowo rozwiązań oferowanych przez metodykę PRINCE2, a jedynie wykorzystywało jej elementy, m.in.: opracowywano i prowadzono analizy ryzyka, rejestr ryzyka, harmonogram, odbiory

26 Ang. *Managing Successful Programmes.*

27 Ang. *Projects in Controlled Environment.*

28 Zarządzenie Nr 43 Ministra Spraw Wewnętrznych z dnia 15 maja 2013 r. w sprawie ustalenia struktury zarządzania projektem „pl.ID" (Dz. Urz. MSW poz. 48), zmienione zarządzeniem Nr 2 Ministra Spraw Wewnętrznych z dnia 22 stycznia 2014 r. (Dz. Urz. MSW poz. 4) i zarządzeniem Nr 21 Ministra Spraw Wewnętrznych z dnia 12 czerwca 2014 r. (Dz. Urz. MSW poz. 39).

29 Centrum Personalizacji Dokumentów jest jednostką budżetową nadzorowaną przez Ministra Spraw Wewnętrznych i Administracji. Realizuje zadania Ministra Spraw Wewnętrznych i Administracji w zakresie wydawania dokumentów dla obywateli polskich, pracowników administracji publicznej, funkcjonariuszy służb podległych Ministrowi Spraw Wewnętrznych i Administracji, cudzoziemców oraz udostępniania danych z rejestru PESEL.

produktów (zleceń), raporty okresowe. Prowadząc harmonogram projektów MSW nie korzystało z narzędzi kontroli postępu prac, jakim są tzw. etapy zarządcze[30]. Pominięto aspekt zarządzania jakością, domyślnie powierzając ją wykonawcy (COI).

W umowie nr 4/DSiA/2013 nie zostały określone przez MSW wymagania odnośnie stosowania przez COI konkretnej metodyki zarządczej. W prace dotyczące budowy SRP zostali zaangażowani pracownicy różnych pionów COI[31]. Ponadto, zostały powołane zespoły odpowiedzialne m.in. za obsługę zarządczą oraz koordynację i wsparcie zadań związanych z wdrożeniem i uruchomieniem SRP.

W procesie zarządzania wytwarzaniem oprogramowania na potrzeby SRP, COI wykorzystywał metodykę *Scrum*. Według wyjaśnień Dyrektora COI, metodyka ta została przyjęta do zarządzania projektem, gdyż pozwalała na dostosowanie się do narzuconych ram czasowych realizacji projektu, skoncentrowanie na istocie wytwarzanego oprogramowania i znanych wymaganiach klienta, ponieważ zakres projektu wielokrotnie ulegał zwiększeniu, bądź zmianom. Stosowana metodyka pozwalała także na utrzymanie motywacji zespołu projektowego. Zastosowanie metodyki *Scrum* przewidziano również do obsługi prac w ramach gwarancji wynikającej z umowy nr 4/DSiA/2013. Dyrektor COI wyjaśnił także, że w procesie wytwarzania oprogramowania wykorzystywano wiele uznanych technik i metod wytwarzania[32] oraz zarządzania jakością kodu źródłowego[33].

Przyjęcie metodyki *Scrum* przez COI było zasadne i pozwalało COI na kontrolowanie zakresu prac programistów i testerów. Stwierdzono jednak, że podczas wytwarzania oprogramowania przedstawiciele MSW nie uczestniczyli regularnie w tzw. spotkaniach *Scrumowych*, mających na celu bieżącą ocenę funkcjonalności opracowanych przez programistów w wytwarzanym oprogramowaniu SRP. Zgodnie z wyjaśnieniami Dyrektor COI, po początkowym okresie współpracy MSW zrezygnowało z udziału w tych spotkaniach; wymagania MSW były przekazywane podczas innych spotkań, tj. analitycznych, prezentacyjnych, organizacyjnych. **Zdaniem NIK, rezygnacja z udziału w spotkaniach *Scrumowych* pozbawiła MSW możliwości bieżącej weryfikacji opracowywanych przez COI elementów i funkcjonalności systemu oraz poprawy zidentyfikowanych usterek lub braków.**

Udostępnienie elementów/funkcjonalności SRP

Pierwotna data udostępnienia SRP, tj. 1 stycznia 2015 r., wynikała z przepisów ustawy Prawo o aktach stanu cywilnego oraz zmian do ustaw o ewidencji ludności i o dowodach osobistych.
Ustawą z dnia 19 grudnia 2014 r. o zmianie ustawy o dowodach osobistych, ustawy o ewidencji ludności oraz ustawy – Prawo o aktach stanu cywilnego, termin udostępnienia SRP został przesunięty na 1 marca 2015 r. MSW potrzebę przesunięcia terminu udostępnienia SRP uzasadniało brakiem gotowości systemu do wdrożenia, m.in. ze względu na zgłaszane przez użytkowników w trakcie testów akceptacyjnych usterki w wytworzonym przez COI oprogramowaniu. W związku ze zmianą terminu udostępnienia systemu na dzień 1 marca 2015 r., na podstawie aneksu nr 3

30 Część projektu, którą Kierownik projektu zarządza w imieniu Komitetu Sterującego w danym czasie. Po jej zakończeniu Komitet Sterujący dokonuje przeglądu dotychczasowych postępów, stanu realizacji Planu projektu, Uzasadnienia Biznesowego oraz ryzyk, a także Planu (następnego) Etapu, w celu podjęcia decyzji, czy projekt należy kontynuować. Źródło: OGC: *Managing Successful Projects with PRINCE2* (2009 ed.), TSO, ISBN 978-0-11-331059-3.

31 Piony: ds. Kluczowych Projektów, Eksploatacji Systemów, Rozwoju Systemów, Rozwoju Produktów i Usług.

32 Np. *Continuous Integration, Test Driven Development, Domain Driven Development*.

33 Np. *pull request*, testy pokrycia.

do umowy nr 4/DSiA/2013 z 28 lutego 2015 r. MSW przesunęło na 28 lutego 2015 r. terminy realizacji zleceń dotyczących ww. elementów SRP, a następnie odebrało jedynie warunkowo od COI prace w tym zakresie, ze względu na stwierdzone problemy i błędy, które jednak nie miały charakteru krytycznego.

Kierownicy poszczególnych projektów w MSW prowadzonych w ramach programu *pl.ID*, wśród problemów zaistniałych w trakcie realizacji SRP wskazali[34] m.in.:

- liczne usterki w oprogramowaniu COI zidentyfikowane przez użytkowników podczas testów akceptacyjnych,
- brak realizacji przez COI części wymagań funkcjonalnych i niefunkcjonalnych wynikających z projektów technicznych,
- problemy we współpracy komponentów systemu,
- zgłaszanie przez użytkowników dodatkowych wymagań co do funkcjonalności w trakcie testów oprogramowania,
- brak opracowania ostatecznych zapisów ustawy Prawo o aktach stanu cywilnego i aktów wykonawczych do ustawy, uniemożliwiający dokładne określenie wymagań dla rejestracji stanu cywilnego.

SRP został uruchomiony z dniem 1 marca 2015 r., jednak na ten dzień nadal istniały w nim liczne usterki. Do momentu uruchomienia systemu nie zostały również wdrożone zalecenia zawarte w ekspertyzie wykonanej na zlecenie MSW w grudniu 2014 r., dotyczącej spełniania przez SRP wymogów funkcjonalnych i wydajnościowych oraz systemu zarządzania zmianą, ryzykiem i ciągłością działania po stronie COI. W ekspertyzie został przedstawiony wykaz 10 obserwacji (spostrzeżeń usterek i nieprawidłowości lub uwag) wskazujących na zasadnicze problemy, których nierozwiązanie mogło spowodować poważne trudności w eksploatacji SRP i znacząco obniżać jakość systemu. Rekomendacje przedstawione w ww. ekspertyzie nie mogły być wzięte przez COI pod uwagę, ze względu na jej przekazanie przez MSW do COI po raz pierwszy dopiero w styczniu 2016 r. Ekspertyza opierała się jedynie na dokumentacji, której najpóźniejszy dokument datowany był na 15 grudnia 2014 r., tak więc na początku 2016 r. większość rekomendacji była nieaktualna, a część niezasadna. Powyższe potwierdziła Minister Cyfryzacji.

Po uruchomieniu SRP 1 marca 2015 r. COI sukcesywnie wprowadzał poprawki do systemu w oparciu o zestawione w tzw. „raportach rozbieżności" błędy i braki.

Ostateczny odbiór prac COI (wynikających z umowy nr 4/DSiA/2013) nastąpił 31 grudnia 2015 r. Przyjęty przez MSW termin realizacji SRP (31 grudnia 2015 r.) wynikał przede wszystkim z faktu, że był on finansowany z wykorzystaniem dofinansowania UE na lata 2007–2013, w związku z czym okres kwalifikowalności dla wydatków związanych z realizacją systemu upływał z dniem 31 grudnia 2015 r.

Z wyjaśnień Dyrektor COI wynika, że do momentu uruchomienia SRP zakres prac projektowych był rozszerzany przez MSW, wprowadzane były zmiany w wymaganiach, np. zmiany wynikające z faktu, że przepisy dotyczące prawa o aktach stanu cywilnego były tworzone równolegle z powstającym oprogramowaniem. W ocenie Kierownika Projektu w COI, zakres wymagań dla Bazy Usług Stanu Cywilnego został zwiększony o około 2/3 w stosunku do pierwotnych założeń. Ponadto, według wyjaśnień Dyrektora COI, dotyczących

[34] W raportach końcowych dla poszczególnych projektów w ramach programu *pl.ID*.

realizacji napraw wynikających z raportów rozbieżności, *(…) W trakcie realizacji zmian MSW zgłosiło oczekiwania dotyczące wdrożenia innych zmian niż wskazano w Raportach Rozbieżności z 28 lutego 2015 r. W związku z tym sporządzając Protokoły Odbioru Produktu (…) dokonano aktualizacji Raportów Rozbieżności (…).*

Podsekretarz Stanu w MSWiA podał, że *(…) Pierwotny termin uruchomienia Systemu Rejestrów Państwowych (SRP) został zaplanowany na dzień 1 stycznia 2015 r. (…) Minister Spraw Wewnętrznych podjął działania mające na celu przesunięcie tego terminu. W uzasadnieniu do projektu ustawy (…) wskazano, że: „Celem projektu ustawy o zmianie ustawy o dowodach osobistych, ustawy o ewidencji ludności oraz ustawy – Prawo o aktach stanu cywilnego (…) jest zapewnienie bezpiecznego, tj. bez negatywnych skutków dla obsługi obywateli, wdrożenia Systemu Rejestrów Państwowych (…) dodatkowy czas pozwoli na kolejną weryfikację działania zbudowanych systemów, umożliwi także lepsze przygotowanie urzędników do obsługi nowych rejestrów i dokonanie zmian w organizacji pracy urzędów. (…) Przesunięcie terminu pozwoli na dodatkową weryfikację pracy zbudowanych systemów również z punktu widzenia bezpieczeństwa danych (…)".* Ponadto poinformował, że *(…) Kolejnej próby przesunięcia tego terminu nie podejmowano, mimo że 28 lutego 2015 r. rejestry zostały odebrane warunkowo. (…) istniejące wciąż błędy nie uniemożliwiały pracy w rejestrze stanu cywilnego (…). Dodatkowo na etapie prac parlamentarnych z poparciem ministra właściwego do spraw wewnętrznych, wprowadzono do ustawy – Prawo o aktach stanu cywilnego 6-cio miesięczny okres przejściowy zakładający możliwość realizacji zadań przez kierowników urzędu stanu cywilnego na podstawie przepisów dotychczasowych.*

Przed uruchomieniem SRP nie zostało przeprowadzone przez COI wdrożenie pilotażowe tego systemu. Działania takiego MSW nie przewidziało w harmonogramie programu *pl.ID*, jednak w grudniu 2014 r., po podjęciu przez MSW decyzji o przesunięciu wdrożenia SRP z 1 stycznia 2015 r. na 1 marca 2015 r. pojawiła się sugestia MSW przeprowadzenia takiego wdrożenia w ograniczonej liczbie gmin. Ostatecznie w styczniu 2015 r. MSW podjęło decyzję o przeprowadzeniu we wszystkich gminach, przy udziale COI, weryfikacji poprawności połączenia z SRP za pośrednictwem dedykowanej sieci teleinformatycznej OST 112 oraz uwierzytelnień użytkowników i aktualności certyfikatów. Jak wyjaśnił Dyrektor COI, działania te nie miały waloru wdrożenia pilotażowego SRP, ponieważ użytkownicy końcowi nie podejmowali faktycznej pracy na rzeczywistych danych i nie wykonywali formalnych czynności urzędowych w systemie.

Według NIK, uwzględnienie przez MSW w procesie wytwarzania SRP przez COI wdrożenia pilotażowego pozwoliłoby na przetestowanie systemu w praktyce oraz umożliwiłoby ujawnienie i wyeliminowanie szeregu błędów oraz braków w funkcjonalnościach systemu jeszcze przed finalnym udostępnieniem go użytkownikom końcowym.

Pomimo przesunięcia terminu udostępnienia SRP na 1 marca 2015 r. w systemie nadal występowały braki i błędy , o czym świadczy liczba i skala problemów, które ujawniły się już po uruchomieniu SRP.

Problemy z funkcjonowaniem SRP po jego uruchomieniu 1 marca 2015 r.

Na podstawie badania próby losowo wybranych 3 tys. zgłoszeń użytkowników SRP zarejestrowanych w prowadzonym przez COI systemie ITSM *Atmosfera*, stanowiących 7,5% wszystkich zgłoszeń (40 197) zarejestrowanych w okresie od 1 marca 2015 r. do 15 czerwca 2016 r., ustalono, że najczęściej powtarzającymi się problemami związanymi z funkcjonowaniem SRP były:

– błędy systemu w trakcie wykonywania różnych działań (np. komunikat o błędzie technicznym 500);
– problemy dotyczące dostępu do aplikacji „Źródło" (np. błędna konfiguracja stacji roboczych, w szczególności konfiguracja certyfikatów);
– problemy wynikające z braku migracji aktów stanu cywilnego do Bazy Usług Stanu Cywilnego;
– problemy z wykonywaniem działań ze względu na braki danych w rejestrze;
– awarie łącza teleinformatycznego wykorzystywanego na potrzeby SRP (problem z połączeniem się lub z komunikacją z SRP poprzez aplikację „Źródło");
– problemy z dostępnością systemu (przedłużające się prace modernizacyjne i problemy będące następstwem wprowadzenia aktualizacji);
– problemy z wykonywaniem czynności wskutek braku spójności danych (np. różne daty wydania/odbioru tego samego dokumentu w rejestrach);
– problemy z wykonywaniem czynności ze względu na nieintuicyjną obsługę systemu;
– problemy związane ze sprzętem (np. nieprawidłowe działanie skanera);
– powolne działanie systemu (tzw. problemy wydajnościowe).

Według danych COI, do 17 czerwca 2016 r. w ramach gwarancji w COI zostało rozwiązanych i zamkniętych 15,3 tys. zgłoszeń użytkowników, zarejestrowanych w systemie ITSM *Atmosfera*.

Na konieczność usprawnienia aplikacji „Źródło" wskazywano też w 13 kontrolowanych urzędach miast/miast i gmin, gdzie stwierdzono m.in., że wprowadzenie aplikacji „Źródło" powodowało niekiedy pogorszenie i wydłużenie czasu obsługi obywateli, m.in. ze względu na:
– konieczność przebudowywania wzmianek na aktach migrowanych na strukturę określoną w systemie SRP, co oznacza, że wpis w akcie nie może być przeniesiony w dotychczasowej treści;
– brak powiązań słowników powoduje, że wiele pól trzeba uzupełniać ręcznie, podczas gdy system mógłby to robić automatycznie (np. gdy w akcie wpisuje się imię dziecka „Jan", to automatycznie powinno wypełnić się pole „płeć" i „stan cywilny", jeżeli wybiera się ze słownika miasto „Warszawa" to system powinien sam wypełnić pole „kraj");
– brak możliwości pobierania danych z Bazy Usług Stanu Cywilnego do tworzonych aktów stanu cywilnego (np. brak możliwości przeniesienia danych rodziców z aktu małżeństwa do projektu aktu urodzenia dziecka);
– brak możliwości jednoczesnego otwarcia okien „PESEL" i „BUSC";
– brak automatycznego dodawania przypisków w istniejących już aktach stanu cywilnego np. przy tworzeniu aktu urodzenia dziecka i zamieszczeniu w nim przypisku o zawarciu małżeństwa przez rodziców, krzyżowo powinien pojawić się przypisek w akcie małżeństwa rodziców o akcie urodzenia dziecka;
– brak możliwości poprawienia oczywistego błędu z już podpisanego aktu przez kierownika USC;
– brak możliwości seryjnego wydruku odpisów, bez konieczności każdorazowego przechodzenia przez te same czynności, co znacznie wydłuża oczekiwanie obywatela na wydanie odpisów aktów stanu cywilnego;
– brak możliwości dodawania we wzmiankach znaków specjalnych, jak np. „§" (pracownicy USC kopiują je z plików tekstowych);
– brak podstawy prawnej we wzorcu wzmianki o sprostowaniu lub uzupełnieniu aktu (za każdym razem trzeba ją wpisywać);
– samoczynne zmiany przez aplikację nazwy organu wydającego dowód osobisty;

– brak możliwości wydruku potwierdzenia złożenia wniosku o wydanie dowodu osobistego (pomimo wybrania opcji „wydrukuj" potwierdzenie to nie było drukowane, a aplikacja informowała, że dokument został już wydrukowany i uniemożliwiała jego ponowny wydruk – powodowało to konieczność wydawania potwierdzeń sporządzanych odręcznie).

Jedną z głównych przyczyn wystąpienia ww. problemów był brak wdrożenia pilotażowego SRP.

Minister Cyfryzacji poinformowała, że *(…) w prowadzonym wspólnie dla wszystkich realizowanych projektów/komponentów wchodzących w zakres Programu pl.ID rejestrze ryzyk, Biuro Programu pl.ID na bieżąco odnotowywało zgłaszane problemy mogące mieć wpływ na uruchomienie SRP i tym samym obsługę obywateli. Materiał był przekazywany osobom zaangażowanym w realizację Programu, w tym właścicielowi Programu, w randze Podsekretarza Stanu MSW. Jako przykład można podać projekt SRP, w czasie trwania którego (od dnia 8 lipca 2013 r.) wykryto i zgłoszono 14 ryzyk, z czego wszystkie zostały zamknięte. Podobnie w projekcie RSC, wszystkie ryzyka zostały zamknięte, jakkolwiek niektóre z nich zmaterializowały się i koniecznym było podjęcie odpowiednich działań naprawczych. Niezbędnym okazało się również przesunięcie daty wejścia w życie ustawy – Prawo o aktach stanu cywilnego o dwa miesiące z uwagi na fakt, że w dniu 1 stycznia 2015 r. narzędzie do prowadzenia elektronicznej rejestracji stanu cywilnego nie było jeszcze gotowe.*

W celu eliminacji pojawiających się po uruchomieniu SRP problemów COI realizowało prace naprawcze w ramach gwarancji do umowy nr 4/DSiA/2013. MC uzgodniło z COI wykonanie 180 poprawek w ramach gwarancji, w tym zmiany dotyczące ergonomii pracy w systemie oraz integrację pomiędzy rejestrami wchodzącymi w skład SRP.

Prace związane z rozwojem oprogramowania SRP

Od momentu uruchomienia SRP, COI współpracował w trybie roboczym z MSW w zakresie prac rozwojowych, brak było formalnego zlecenia tego typu prac, a COI obsługiwał jedynie zgłoszenia mieszczące się w ramach gwarancji umownej. W 2015 r. w wyniku współpracy COI i MSW zostało zdefiniowanych ponad 220 zagadnień stanowiących rozszerzenia i ulepszenia funkcji SRP. W 2015 r. zostało również zorganizowane przez MSW spotkanie z przedstawicielami jednostek samorządu terytorialnego, dotyczące zagadnień związanych z rozwojem i standaryzacją budowy sieci SRP, bezpieczeństwem stacji końcowych, aktualizacją oprogramowania i doposażeniem urzędów. Utworzono forum internetowe w celu komunikacji i pomocy w ww. zakresie. W systemie ITSM *Atmosfera* została uruchomiona usługa umożliwiająca rejestrację przez użytkowników propozycji rozwojowych i udoskonaleń. W okresie marzec-sierpień 2015 r. COI przeprowadził cykl spotkań w pięciu USC w celu weryfikacji poprawności i efektywności działania BUSC oraz zebrania propozycji zmian w systemie.

W 2016 r. została zintensyfikowana współpraca robocza pomiędzy COI i MC oraz użytkownikami końcowymi w zakresie rozwoju SRP. Minister Cyfryzacji poinformowała, że *(…) podjęto pilne działania mające na celu optymalizację działania systemu. Ministerstwo Cyfryzacji przeprowadziło spotkania z użytkownikami oraz konsultacje w zakresie rozwoju SRP. (…) W zakresie określenia wymagań dotyczących rozwoju SRP MC przyjęło koncepcję, której głównym założeniem była ścisła współpraca z użytkownikami końcowymi systemu w zakresie wszystkich komponentów SRP (…) Użytkownicy zostali włączeni w cały proces produkcji oprogramowania – od analiz aż po testy akceptacyjne. (…) Dla każdego ze wskazanych komponentów, tj. BUSC, RDO, PESEL oraz KN, MC powołało grupy*

robocze, przy czym w skład każdej z nich wchodzi około 10 osób. Grupę roboczą tworzy stały zespół osób, zaangażowanych w prace projektowe nad danym komponentem. W skład takich grup wchodzą przedstawiciele MC, COI oraz użytkowników końcowych. (…) Do głównych zadań grupy roboczej należy:

- *ustalenie ostatecznego zakresu zmian funkcjonalnych w ramach danego etapu prac projektowych,*
- *określanie priorytetów w ramach danego etapu prac projektowych,*
- *definiowanie i akceptacja szczegółowych wymagań funkcjonalnych dla danej zmiany,*
- *terminowa realizacja zadań ustalonych na spotkaniach grupy roboczej,*
- *potwierdzanie poprawności wdrożonych rozwiązań funkcjonalnych podczas testów akceptacyjnych.*

Do 16 czerwca 2016 r. przeprowadzono łącznie osiem spotkań grup roboczych z udziałem przedstawicieli COI.

Prace rozwojowe dotyczące SRP opierają się na katalogu zmian zweryfikowanych pod kątem formalno-prawnym i wykonalności technicznej przez MC i COI. Według informacji przekazanej przez Minister Cyfryzacji, na czerwiec 2016 r. katalog ten obejmował ponad 350 propozycji, z czego ok. 40% dotyczyło BUSC i był on na bieżąco aktualizowany. Odpowiedzi na zgłaszane przez użytkowników propozycje zmian były publikowane przez COI na stronie internetowej[35] i przekazywane do dalszych prac. Poszczególnym zmianom nadawano priorytet pilności realizacji.

Działania polegające na aktywnym włączeniu użytkowników końcowych w prace rozwojowe oprogramowania SRP mogą wpłynąć na wyeliminowanie szeregu błędów zidentyfikowanych w działaniu systemu, a także ułatwić bieżącą modyfikację SRP w związku ze zmianami w przepisach prawa oraz wpłynąć na poprawę działania poszczególnych funkcjonalności wykorzystywanych przez użytkowników w trakcie obsługi spraw obywateli z wykorzystaniem SRP.

Usługi elektroniczne świadczone z wykorzystaniem SRP

W związku z realizacją programu *pl.ID* COI udostępnił z dniem 1 marca 2015 r. cztery e-usługi:

- *Sprawdź swoje dane w rejestrze PESEL,*
- *Sprawdź, czy dowód jest unieważniony,*
- *Sprawdź swoje dane w Rejestrze Dowodów Osobistych,*
- *Sprawdź, czy dowód osobisty jest gotowy.*

Ponadto, w 2015 r. poprzez stronę internetową www.obywatel.gov.pl zostały udostępnione przez MSW inne e-usługi[36] umożliwiające:

- złożenie wniosku o wydanie dowodu osobistego,
- złożenie wniosku o wydanie odpisu aktu stanu cywilnego,
- zgłoszenie utraty lub uszkodzenia dowodu osobistego.

W okresie od 1 marca 2015 r. do 31 maja 2016 r. do kontrolowanych 13 urzędów miast/miast i gmin wpłynęło drogą elektroniczną 2 106 wniosków o wydanie dowodu osobistego, 1 407 wniosków o wydanie odpisu aktu stanu cywilnego oraz 23 zgłoszenia utraty lub uszkodzenia dowodu osobistego. Szczegółowe dane zawarto w tabeli nr 1.

[35] https://www.coi.gov.pl/artykul/kolejne-propozycje-rozwoju-srp.html

[36] Usługi te nie wykorzystują bezpośrednio SRP, powstały one poza zakresem programu *pl.ID*.

Tabela nr 1
Liczba wniosków wpływających do kontrolowanych urzędów miast/miast i gmin w formie elektronicznej w okresie od 1 marca 2015 r. do 31 maja 2016 r.

Nazwa jednostki objętej kontrolą	Liczba wniosków o wydanie dowodu osobistego	Liczba zgłoszeń utraty lub uszkodzenia dowodu osobistego	Liczba wniosków o wydanie odpisu aktu stanu cywilnego
Urząd Miejski Wrocławia	1353	0	255
Urząd Miejski w Białymstoku	277	15	0
Urząd Miasta i Gminy Piaseczno	108	0	11
Urząd Miasta Stołecznego Warszawy – Urząd Dzielnicy Ochota	108	0	1084
Urząd Miasta Rzeszowa	102	4	15
Urząd Miasta w Wałbrzychu	37	0	13
Urząd Miejski w Świdnicy	28	0	7
Urząd Miasta Legionowo	25	1	5
Urząd Miasta Otwocka	24	3	6
Urząd Miejski w Łomży	21	0	0
Urząd Miejski w Przemyślu	20	0	11
Urząd Miasta Bielsk Podlaski	3	0	0
Urząd Miasta Krosna	0	0	0

Źródło: Wyniki kontroli NIK.

W związku z realizacją usługi elektronicznej w zakresie złożenia wniosków o wydanie dowodu osobistego, badaniem objęto łącznie próbę 79 wniosków. Stwierdzono, że w pięciu[37] z 13 kontrolowanych urzędów wnioskodawcom nie przekazywano *potwierdzenia złożenia wniosku o wydanie dowodu osobistego*, co było niezgodne z § 10 ust. 4 rozporządzenia Ministra Spraw Wewnętrznych z dnia 29 stycznia 2015 r. w sprawie wzoru dowodu osobistego oraz sposobu i trybu postępowania w sprawach wydawania dowodów osobistych, ich utraty, uszkodzenia, unieważnienia i zwrotu[38]. Nieprawidłowość tą tłumaczono m.in. niedopatrzeniem.

Unieważnianie dowodu osobistego z wykorzystaniem SRP

Badaniem objęto automatyczne unieważnianie dowodu osobistego w RDO w chwili wprowadzenia do SRP informacji o zgonie obywatela. Analizie poddano 441,6 tys. danych o zgonach obywateli[39] mających miejsce w okresie od 1 marca 2015 r. do 31 maja 2016 r.[40]. W 1 601 przypadkach w RDO nie zawarto informacji o unieważnieniu dowodów osobistych. Minister Cyfryzacji wskazała, że *w rejestrze PESEL jako ostatni wydany dowód osobisty figurował nie aktualny, a poprzedni dowód osobisty danej osoby – zlecenie unieważnienia dowodu osobistego wysyłane z rejestru PESEL do Rejestru*

37 UM (liczba nieprzekazanych *potwierdzeń złożenia wniosku*/liczba badanych wniosków): Bielsk Podlaski (jeden/trzy), Otwock (jeden/sześć), Piaseczno (siedem/siedem), Wrocław (trzy/pięć), Rzeszów (pięć/pięć).

38 Dz. U. poz. 212.

39 Badanie przeprowadzono z wykorzystaniem programu komputerowego ACL służącego do analizy danych.

40 Informację uzyskano w trybie art. 29 ust. 1 pkt 2 lit. f ustawy o NIK z Ministerstwa Cyfryzacji.

Dowodów Osobistych (RDO) zawiera numer PESEL oraz serię i numer dowodu figurującego w rejestrze PESEL. W związku z tym do RDO przesyłane było zlecenie unieważnienia poprzedniego dowodu osobistego, tym samym nie unieważniając właściwego ostatnio wydanego dowodu osobistego. Minister Cyfryzacji poinformowała, że wymienione przypadki aktualnie już nie występują (…) *gdyż zostały wyeliminowane poprzez przeprowadzenie w październiku 2015 r. procesu wyrównania danych z Rejestru Dowodów Osobistych do rejestru PESEL w zakresie ostatnio wydanego dowodu osobistego.*

3.2 Wpływ wdrażania SRP na sprawność pracy użytkowników w jednostkach samorządu terytorialnego

Migracja danych do SRP

1. Wraz z uruchomieniem SRP z dniem 1 marca 2015 r. nie dokonano w kontrolowanych urzędach miast/miast i gmin masowej migracji aktów stanu cywilnego z dotychczas wykorzystywanych systemów informatycznych obsługujących sprawy z zakresu aktów stanu cywilnego. W urzędach dokonywano migracji pojedynczych aktów stanu cywilnego w przypadku zleceń migracji otrzymywanych z innych urzędów, dokonywania czynności z zakresu USC lub wydawania odpisu aktu stanu cywilnego dla wnioskodawcy.

Masowa migracja danych została natomiast przewidziana i przeprowadzona m.in. dla rejestrów: PESEL i RDO. Szczegółowe dane w zakresie przeprowadzonej migracji danych zawarto w tabeli nr 2.

Tabela nr 2
Liczba rekordów migrowanych do SRP

Rejestr (moduł SRP), do którego migrowano dane	Liczba rekordów zaimportowanych	Liczba rekordów niezaimportowanych	% rekordów niezaimportowanych
PESEL	502 061 359	454 840	0,1
RDO	160 574 941	770 032	0,5

Źródło: Wyniki kontroli NIK.

Według *Raportu końcowej migracji danych* z dnia 15 maja 2015 r., opracowanego przez COI, brak migracji wszystkich rekordów do poszczególnych rejestrów SRP wynikał m.in. ze słabej jakości danych źródłowych (rozbieżności i braku aktualnych danych) zgromadzonych w dotychczas wykorzystywanych bazach danych.

W ocenie NIK, migracja danych do SRP, w zakresie który został powierzony COI, została przeprowadzona prawidłowo.

Masowa migracja danych z zakresu aktów stanu cywilnego, zgromadzonych w lokalnych systemach informatycznych do BUSC, nie została przewidziana przez MSW w ramach programu *pl.ID*.

Minister Cyfryzacji wskazała, że *(…) głównym powodem braku rozpatrywania procesu masowej migracji aktów stanu cywilnego były w pierwszej kolejności kwestie finansowe, ponieważ nie zostały przewidziane środki na tego typu działanie. Głębsza analiza tematyki masowej migracji realizowana była w momencie, gdy nie była już możliwa zmiana założeń projektowych ze względu na zbyt zaawansowane już wówczas prace programistyczne komponentu BUSC. Kolejny problem dotyczył zaawansowania prac legislacyjnych w przedmiocie uchwalenia ustawy Prawo o aktach stanu*

cywilnego, który wówczas był na ostatniej ścieżce legislacyjnej i nie pozwalał na wprowadzanie kolejnych zmian. Ówczesna ustawa w swoim kształcie nie zawierała przepisów umożliwiających wykonanie procesu masowej migracji. Ciężar procesu w projektowanych przepisach został przeniesiony na kierownika USC, który oprócz swoich ustawowych obowiązków w zakresie rejestracji stanu cywilnego, zobligowany był do brania czynnego udziału w czynności z zakresu migracji. Skutkowało to nałożeniem dodatkowych, względem już wykonywanych, czynności do zrealizowania. Dopiero obecne zmiany legislacyjne, tj.: nowelizacja ustawy z dnia 28 listopada 2014 r. Prawo o aktach stanu cywilnego (wprowadzona ustawą z dnia 6 lipca 2016 r. o zmianie ustawy – Prawo o aktach stanu cywilnego), jak również rozporządzenie Ministra Cyfryzacji z dnia 26 sierpnia br. zmieniające rozporządzenie w sprawie przenoszenia aktów stanu cywilnego do rejestru stanu cywilnego[41] *wprowadziły stosowne zapisy, które umożliwią pełną realizację tego procesu. Przepisy precyzują, że kierownik USC może pisemnie upoważnić pracownika USC do migrowania aktów stanu cywilnego do rejestru stanu cywilnego, tym samym delegując część zadań na upoważnionych pracowników USC.*

W odniesieniu do dodatkowego projektu CASC (*Cyfryzacja Aktów Stanu Cywilnego*), który miał wspierać masową migrację danych z aplikacji lokalnych do SRP, Minister Cyfryzacji podała, że *po produkcyjnym uruchomieniu SRP proces masowej migracji danych o aktach stanu cywilnego do BUSC był wciąż analizowany. Departament Spraw Obywatelskich MSW, jako merytorycznie odpowiedzialny za to zagadnienie, rozpoczął analizę tematu, czego skutkiem było inicjowanie Projektu CASC – Cyfryzacja Aktów Stanu Cywilnego – System Wspierania Migracji w ramach dofinansowania z Programu Operacyjnego Polska Cyfrowa (POPC) działanie 2.1. (…) W dniu 16 października 2015 r. MSW otrzymało z CPPC informację, że projekt CASC uzyskał wynik negatywny i nie został zatwierdzony do realizacji, gdyż nie spełnił kryteriów merytorycznych. W związku z wejściem w życie ustawy z dnia 22 grudnia 2015 r. o zmianie ustawy o działach administracji rządowej oraz niektórych innych ustaw, która z dniem 1 stycznia 2016 r. przeniosła nadzór m.in. nad rejestrem BUSC do MC, Ministerstwo podjęło działania związane z realizacją procesu masowej migracji danych o aktach stanu cywilnego do BUSC. Działania w tym zakresie nie są bezpośrednią kontynuacją założeń projektu CASC, lecz idei procesu masowej migracji. (…) powołana została grupa robocza BUSC, w której pracują zarówno przedstawiciele MC, COI oraz USC, którzy definiują wymagania funkcjonalne i uczestniczą w całym procesie analizy funkcjonalnej wraz z definiowaniem konkretnych rozwiązań w celu jak najlepszego stworzenia narzędzia do masowej migracji danych o aktach stanu cywilnego z aplikacji alternatywnych do BUSC. Zagadnienie to zostało podzielone na dwa etapy, z czego I etap planowany jest do produkcyjnego wdrożenia na grudzień br. Będzie on obejmował rozwiązanie umożliwiające masową migrację danych o aktach z baz lokalnych USC zgromadzonych w aplikacjach alternatywnych do BUSC. II etap natomiast ma obejmować masowe podpisywanie zmigrowanych aktów, co wprowadzi ergonomię przy jednoczesnym przyśpieszeniu całego procesu migracji. Planowany termin realizacji II etapu zakładany jest na pierwszy kwartał 2017 r.*

W czerwcu 2016 r. COI zobowiązał się względem MC do przygotowania narzędzia do masowej migracji danych o aktach stanu cywilnego.

Według NIK, masowa migracja danych z zakresu aktów stanu cywilnego do modułu BUSC, przy wykorzystaniu narzędzia opracowywanego przez COI, jest istotna dla zapewnienia sprawnego załatwiania spraw obywateli przez USC. Przeprowadzenie masowej migracji umożliwiłoby wykorzystanie danych elektronicznych zgromadzonych w lokalnych

[41] Dz. U. poz. 1352.

systemach informatycznych, wykorzystywanych do obsługi aktów stanu cywilnego przed uruchomieniem SRP, bez konieczności ich pojedynczego wprowadzania do SRP, co mogłoby znacznie przyspieszyć obsługę obywateli. W poszczególnych urzędach stanu cywilnego przed 1 marca 2015 r. wykorzystywano lokalne aplikacje wspierające proces rejestracji zdarzeń stanu cywilnego, jednak mając na uwadze, że nie istniały wówczas normy prawne, które nakazywałyby ich tworzenie i określałyby sposób ich funkcjonowania, aplikacje te były tworzone i wykorzystywane pomocniczo.

2. Zgodnie z art. 125 ust. 3 p.a.s.c. kierownik urzędu stanu cywilnego, który przechowuje księgę, dokonuje przeniesienia aktu stanu cywilnego do rejestru stanu cywilnego w ciągu 7 dni roboczych od dnia, gdy do niego złożono wniosek o wydanie odpisu lub wydanie zaświadczenia. W myśl art. 125 ust. 4 p.a.s.c. kierownik urzędu stanu cywilnego, do którego złożono wniosek o wydanie odpisu lub wydanie zaświadczenia, a księga nie jest przez niego przechowywana, przekazuje wniosek do kierownika urzędu stanu cywilnego przechowującego księgę w terminie umożliwiającym wydanie odpisu lub zaświadczenia w ciągu 10 dni roboczych od dnia złożenia wniosku.

W 13 kontrolowanych urzędach miast/miast i gmin badaniem objęto 396 zleceń migracji aktów stanu cywilnego (wnioski o wydanie odpisów aktów małżeństwa, urodzenia i zgonu) w okresie od 1 marca 2015 r. do 31 lipca 2016 r. Wyniki kontroli wykazały, że:

- w przypadku 170 (ze 180, tj. 94%) wniosków o wydanie odpisu aktu stanu cywilnego z ksiąg przechowywanych w kontrolowanych urzędach, migracja aktu do rejestru stanu cywilnego w aplikacji „Źródło" w kontrolowanym urzędzie następowała do 7 dni roboczych od dnia złożenia wniosku przez obywatela, tj. zgodnie z art. 125 ust. 3 p.a.s.c. W przypadku 10 wniosków[42] migracja nastąpiła z przekroczeniem terminu wskazanego w art. 125 ust. 3 p.a.s.c.;
- w 17 przypadkach zlecenie migracji aktów stanu cywilnego do SRP[43] nie było niezbędne, gdyż pięć aktów było już zmigrowanych do SRP, a 12 odpisów tych aktów zostało wydanych na podstawie przepisów przejściowych[44];
- w przypadku 193 (z 199, tj. 97%) wniosków o wydanie odpisu aktu stanu cywilnego z ksiąg stanu cywilnego nieprzechowywanych w kontrolowanych urzędach, zlecono migrację aktu innemu właściwemu urzędowi zazwyczaj w terminie jednego dnia roboczego od złożeniu wniosku. W przypadku sześciu wniosków[45], zlecenie innemu urzędowi migracji aktów stanu cywilnego następowało po upływie 10 dni i więcej, uniemożliwiając tym samym wydanie przez kontrolowany urząd odpisów w terminie 10 dni roboczych, o którym mowa w art. 125 ust. 4 p.a.s.c.

Kontrolą objęto także realizację zleceń migracji aktów stanu cywilnego wpływających z innych urzędów. Z 3 913 zleceń migracji poddanych kontroli, 284 zlecenia (tj. 7%) zrealizowano z przekroczeniem terminu określonego w art. 125 ust. 4 p.a.s.c. Przyczynami opóźnień w realizacji zleceń migracji były m.in.:

42 UM (liczba wniosków, dla których migracja danych nastąpiła powyżej 7 dni roboczych od dnia złożenia): Wałbrzych (1), Warszawa (6), Wrocław (3).

43 UM: Białystok, Łomża, Piaseczno.

44 Art. 145 p.a.s.c. umożliwiał kierownikowi urzędu stanu cywilnego wykorzystanie dotychczasowych aplikacji do rejestracji stanu cywilnego przez okres 6 miesięcy od dnia wejścia w życie p.a.s.c, tj. od dnia 1 marca 2015 r. do dnia 31 sierpnia 2015 r.

45 UM (liczba wniosków, dla których zlecenie migracji danych innemu urzędowi nastąpiło powyżej 10 dni roboczych od dnia złożenia wniosków): Białystok (2), Łomża (1), Wałbrzych (1), Warszawa (1), Wrocław (1).

– dowolność wyboru urzędu stanu cywilnego, w którym ma nastąpić dokonanie czynności, co spowodowało zwiększenie liczby wniosków wpływających do kontrolowanych USC;
– udostępnienie urzędom stanu cywilnego pustej bazy danych w aplikacji „Źródło", co uniemożliwiało korzystanie z danych z innych USC;
– bardzo wolne funkcjonowanie aplikacji „Źródło" w początkowym okresie (długa praca przy przetwarzaniu danych, zawieszanie się aplikacji i inne błędy).

Wydłużało to czas obsługi interesanta i załatwiania wszystkich innych czynności. Opóźnienia w realizacji zleceń migracji miały miejsce w sześciu z 13 kontrolowanych urzędów[46], gdyż wprowadzanie do aplikacji „Źródło" danych w zakresie aktów stanu cywilnego następowało po 10 dniach od dnia otrzymania zlecenia z innego urzędu. Uniemożliwiało to wydanie obywatelowi odpisu aktu stanu cywilnego w terminie 10 dni od dnia złożenia przez niego wniosku i stanowiło naruszenie art. 125 ust. 4 p.a.s.c. Na przykład:

- W **Urzędzie m.st. Warszawy** nieterminowo zrealizowano 220 z 300 poddanych kontroli zleceń migracji wpływających z innego urzędu (co stanowiło 73% zleceń objętych kontrolą). Zlecenia te zostały zrealizowane przez USC m.st. Warszawy w terminie od 11 do 178 dni roboczych. W celu poprawy obsługi obywateli oraz terminowości załatwiania spraw w USC m.st. Warszawy zwiększono zatrudnienie oraz wprowadzono „system przyśpieszeń" dla migracji aktów, których odpisy są niezbędne mieszkańcom do załatwienia spraw losowych, niecierpiących zwłoki. Ponadto, awansowano 10 pracowników na stanowiska zastępców kierownika USC, aby więcej osób mogło zatwierdzać akty i odpisy, a także wystąpiono do MSWiA o rozpatrzenie możliwości nowelizacji ustawy w zakresie wydawania odpisów z aplikacji wspierającej.
- W **Urzędzie Miasta i Gminy Piaseczno** nieterminowo zrealizowano 17 z 301 poddanych kontroli zleceń migracji z innego urzędu (co stanowiło 6% zleceń objętych kontrolą). Zlecenia te zostały zrealizowane przez USC w Piasecznie w terminie od 11 do 33 dni roboczych.

Nie uwzględnienie przez MSW na etapie przygotowywania projektu *pl.ID*, przeprowadzenia masowej migracji aktów stanu cywilnego do SRP z lokalnych aplikacji wykorzystywanych w USC, skutkowało opóźnieniami w wydawaniu obywatelom odpisów aktów stanu cywilnego, szczególnie w dużych ośrodkach miejskich. Opóźnienia te mogą ulec zmniejszeniu w związku z wprowadzoną przez Sejm, z inicjatywy MC nowelizacją ustawy p.a.s.c.[47], która weszła w życie z dniem 27 sierpnia 2016 r. Zmiany w przepisach umożliwiają m.in. sprawniejsze przenoszenie do rejestru stanu cywilnego aktów sporządzonych w papierowych księgach, dzięki uprawnieniu kierownika USC do upoważnienia pracowników do dokonania tej czynności. Zmiany te umożliwiły również tymczasowe wydawanie przez pięć lat odpisów aktów stanu cywilnego na podstawie danych z lokalnych aplikacji wykorzystywanych w USC przed 1 marca 2015 r.

Zapewnienie sprawnego działania SRP

1. W dniu 30 czerwca 2016 r. pomiędzy MC a COI zawarta została umowa ramowa m.in. na świadczenie usług zapewniających poprawne i nieprzerwane funkcjonowanie SRP. Umowa została zawarta na okres od 1 lipca 2016 r. do 30 czerwca 2019 r. Wcześniej, w okresie od 1 marca 2015 r. do 30 czerwca 2016 r., COI utrzymywało SRP na podstawie czterech umów zawartych z MSW

[46] UM (w nawiasie: liczba zleceń migracji aktów stanu cywilnego otrzymanych od innego urzędu zrealizowanych powyżej 10 dni roboczych od dnia wpływu zlecenia/łączna liczba badanych zleceń migracji): Łomża (17/300), Piaseczno (17/301), Przemyśl (6/300), Wałbrzych (23/300), Warszawa (220/300), Wrocław (1/300).

[47] Ustawa z dnia 6 lipca 2016 r. o zmianie ustawy Prawo o aktach stanu cywilnego (Dz. U. poz. 1221).

i MSWiA. Minimalna dostępność SRP została określona na poziomie 98%. W umowie z 30 czerwca 2016 r. zostały zdefiniowane minimalne wymagania Ministerstwa Cyfryzacji w odniesieniu do poziomu utrzymania SRP. I tak:

- dla procesu zarządzania incydentami określono maksymalny czas na rozwiązanie problemu wynoszący:
  - 3 dni robocze dla incydentu krytycznego (całkowita niedostępność funkcji jednego z modułów, dla którego nie ma obejścia i został zgłoszony przez co najmniej 5% lokalizacji);
  - 10 dni roboczych dla incydentu pilnego (niedostępność systemu i jego usług w co najmniej jednej lokalizacji);
  - 20 dni dla incydentu standardowego (nie powoduje niedostępności usług, ale oznacza ich nieprawidłowe działanie);
- dla procesu zarządzania problemem określono maksymalny czas jego obsługi wynoszący:
  - 40 dni roboczych dla problemu krytycznego,
  - 80 dni roboczych dla problemu pilnego,
  - 120 dni dla problemu standardowego,
- dla usługi serwisu oprogramowania określono gwarantowany czas naprawy błędów w nim stwierdzonych wynoszący:
  - 2 dni robocze dla błędu krytycznego,
  - 12 dni roboczych dla błędu pilnego,
  - 40 dni roboczych dla błędu standardowego.

Według NIK, ustalone w umowie na utrzymanie SRP okresy rozwiązywania i usuwania incydentów (problemów) związanych z funkcjonowaniem SRP są zbyt długie. W takim stanie rzeczy wystąpienie krytycznego incydentu w funkcjonowaniu SRP może powodować w skali kraju trzydniową przerwę, uniemożliwiającą bieżącą rejestrację w SRP narodzin, małżeństw czy zgonów.

2. W dokumencie COI pn. *Procedury eksploatacyjne SRP* określony został sposób monitorowania działania SRP. W myśl tych zapisów monitorowaniu podlega w szczególności:

- działanie serwisów systemów operacyjnych,
- dostęp do SRP pod kątem poszukiwania nieuprawnionych użytkowników lub prób włamań,
- stan działania aplikacji umożliwiających działanie SRP,
- bazy danych.

W COI monitoring działania SRP prowadzony jest przez Zespół Utrzymania Systemów, który przez 24 godziny na dobę monitoruje SRP i podejmuje działania, reagując na zdarzenia zachodzące w systemie.

3. Na zapewnienie dostępności SRP na zakładanym poziomie 98% wpływ mają: COI oraz podmioty zewnętrzne, które dostarczają na rzecz COI m.in. usługi transmisji danych, serwisu infrastruktury technicznej SRP. Ustalono, że umowy z dostawcami zewnętrznymi (łącznie 19 umów) w większości przypadków przewidują, że awarie mają być usuwane przez wykonawców w ciągu 24 godzin lub do końca następnego dnia roboczego od momentu zgłoszenia awarii; w przypadku dwóch umów awarie powinny być usunięte w ciągu 48 godzin.

W ocenie NIK, poza jednym przypadkiem zawarte przez COI umowy z dostawcami zewnętrznymi m.in. na dostawę sprzętu wraz ze wsparciem technicznym oraz na świadczenie

usług telekomunikacyjnych należycie zabezpieczają interesy COI, gdyż zapewniają możliwość monitorowania jakości dostarczanych usług wraz z możliwością naliczania kar umownych w przypadku niezachowania przez dostawców zamówionych parametrów tych usług.

W dniu 5 lutego 2014 r. Minister Spraw Wewnętrznych zawarł porozumienie z Komendantem Głównym Policji, którego przedmiotem było oddanie w użyczenie dla potrzeb SRP powierzchni w pomieszczeniu serwerowni oraz dwóch pomieszczeń biurowo-technicznych. W umowie określono m.in., że Minister Spraw Wewnętrznych ponosi koszty instalacji i napraw urządzeń serwerowni SRP oraz zapewnia ich sprawność i bezpieczeństwo. W umowie tej nie określono parametrów SLA dla pomieszczenia serwerowni (np. w odniesieniu do systemu nieprzerwanego zasilania, kontroli dostępu, klimatyzacji, zabezpieczeń przeciwpożarowych). Również w porozumieniu z dnia 29 czerwca 2016 r. zawartym pomiędzy MC a MSWiA, dotyczącym wykorzystania serwerowni na potrzeby SRP, nie wskazano parametrów SLA. Na podstawie zleceń udzielonych przez MSW w ramach umowy nr 4/DSiA/2013, COI dostarczył wyposażenie serwerowni. Serwerownie posiadają niezależne źródła zasilania zewnętrznego, zapasowe generatory, zasilacze awaryjne; dostarczanie zasilania i chłodzenia jest realizowane niezależnymi traktami.

COI administruje systemami, których właścicielem jest MC, ale nie odpowiada w ramach zawartych umów za serwerownie, w tym za zapewnienie przestrzeni serwerowni, za zasilanie, za nadzór (bezpieczeństwo fizyczne), ani za żadne inne warunki (np. zapewnienie klimatyzacji). MC zapewnia serwerownie i jest właścicielem całej infrastruktury informatycznej, a COI nią administruje i zapewnia serwis dla sprzętu.

NIK zwraca uwagę, że brak wskazania w umowach użyczenia powierzchni serwerowni na rzecz SRP parametrów technicznych SLA może utrudnić COI zapewnienie dostępności SRP na zamówionym przez MC poziomie 98%. Aby mieć możliwość utrzymania dostępności SRP na określonym poziomie, COI powinien dążyć do uregulowania minimalnego poziomu dostępności serwerowni użyczonych przez MSWiA i Policję.

Na potrzeby SRP wykorzystywano sieć OST 112, której operatorem była Policja. Na podstawie umowy z 20 listopada 2014 r. zawartej pomiędzy Ministrem Spraw Wewnętrznych a EXATEL S.A.[48] zapewnienie prawidłowego działania łączy dostępowych do OST 112 dla użytkowników SRP było w gestii firmy EXATEL S.A. Parametry dostępności sieci OST 112 określono w załączniku nr 9 do ww. umowy. Dla ośmiu typów łącz tworzących sieć OST 112 określono maksymalny łączny czas niedostępność sieci, który wynosi od 360 do 1 200 minut miesięcznie, co oznacza, że łącza te powinny być dostępne odpowiednio od 97,22% do 99,17% w ciągu miesiąca. Ustalono, że faktyczny poziom dostępności sieci OST 112 w badanym okresie, tj. od 1 marca 2015 r. do 31 lipca 2016 r. kształtował się na poziomie powyżej 98%, za wyjątkiem czterech miesięcy w 2015 r., w których poziom ten uległ obniżeniu. I tak, w maju wyniósł 92,36%, w czerwcu 97,75%, w lipcu 90,51%, natomiast we wrześniu 97,29%. Obniżona dostępność sieci OST 112 spowodowana była problemami z łączami. Wszelkie problemy związane z działaniem sieci OST 112 zgłaszane były przez COI do MSWiA.

4. W załączniku nr 2 do umowy zawartej w dniu 30 czerwca 2016 r. pomiędzy COI i MC na utrzymanie SRP nr 2/DIT/U/COI/2016 pn. *Katalog Usług Systemu Informatycznego SRP* określono minimalną dostępność (na poziomie 98%) dla wszystkich usług realizowanych w ramach SRP

[48] Nr BAF-VI-2374-2-5/5-TK/2014 ze zm.

oraz parametry czasowe świadczenia poszczególnych usług. COI w okresie od marca 2015 r. sporządzał dla Ministerstwa Spraw Wewnętrznych (od stycznia 2016 r. dla Ministerstwa Cyfryzacji) comiesięczne raporty dostępności poszczególnych usług SRP. Raporty za okres marzec–maj 2015 r. nie zawierały łącznych danych dotyczących dostępności całego SRP, prezentowały natomiast dostępność każdej z 205 usług tworzących SRP. W przypadku dziewięciu z 205 usług w okresie kwiecień–maj 2015 r. ich dostępność wyniosła poniżej 98%[49].

Raporty za okres od czerwca 2015 r. do lipca 2016 r. wskazywały, że dostępność SRP kształtowała się na poziomie od 99,93% do 100%. **NIK zauważa, że osiągnięta dostępność SRP nie oznacza, że działanie systemu było wolne od usterek/błędów, tylko że jego funkcje lub usługi były dostępne.**

Analiza incydentów zgłoszonych w okresie od 1 marca 2015 r. do 15 czerwca 2016 r. wykazała, iż miesięczne raporty z wykonania usług SRP sporządzane w COI nie uwzględniały niektórych incydentów. Na przykład opisane w raporcie za miesiąc kwiecień 2015 r. obniżenie dostępności usługi *Personalizacja blankietów* dotyczyło zgłoszenia, które zostało zarejestrowane 6 marca 2015 r., problem został rozwiązany 18 kwietnia 2015 r., a zamknięcie zgłoszenia nastąpiło 28 kwietnia 2015 r. Wynika z tego, że obniżona dostępność usługi *Personalizacja blankietów* występowała w okresie od 6 marca do 18 kwietnia 2015 r., natomiast w raporcie za marzec 2015 r. dostępność tej usługi została określona na 100%. Nieścisłość wystąpiła także w przypadku obniżenia dostępności usługi *Obsługa działań administracyjnych* w raporcie za maj 2015 r. W tym przypadku zgłoszenie zostało zarejestrowane już 12 marca 2015 r. (rozwiązane i zamknięte 4 maja 2015 r.), a w raporcie za marzec 2015 r. dostępność tej usługi została określona na poziomie 100%. Stwierdzono jeszcze pięć innych przypadków raportowania bez uwzględnienia incydentów mających znaczenie dla poziomu dostępności SRP[50].

Ponadto, w raportach z usług utrzymania SRP wskazano, że problemy z dostępnością łącza występowały wyłącznie w maju, czerwcu i wrześniu 2015 r., podczas gdy z analizy rejestru incydentów wynika, że problemy z łączem wystąpiły również w marcu i grudniu 2015 r. (ponad 500 zgłoszeń) oraz w kwietniu 2015 r. (ponad 100 zgłoszeń).

Według NIK, COI w miesięcznych raportach z wykonania usług SRP powinno uwzględniać wszystkie czynniki wpływające na poziom dostępności usług SRP.

---

49 W kwietniu 2015 r. dostępność usługi *Personalizacja dokumentów* wyniosła 95,3%; w maju 2015 r. dostępność następujących usług kształtowała się poniżej 98%: *Akceptacja wniosku o wydanie dowodu osobistego* 86,02%, *Personalizacja blankietów* 0%, *Wydawanie dowodów osobistych* 95,01%, *Obsługa migracji akt stanu cywilnego* 95,38%, *Obsługa działań administracyjnych w zakresie zarządzania kontami* 96,89%, *Rejestracja zameldowania na pobyt stały* 97,68%, *Przyjmowanie dowodu osobistego* 97,26%, *Łącze dedykowane* 92,36%.

50 **1)** Zgłoszenie 100612 (*Obsługa migracji aktów stanu cywilnego z postaci papierowej do systemu BUSC*), data zgłoszenia: 10 marca 2015 r., data rozwiązania: 30 kwietnia 2015 r., data zamknięcia zgłoszenia: 7 maja 2015 r. – obniżona dostępność usługi uwzględniona jedynie w raporcie za maj 2015 r.; **2)** Zgłoszenie 93813 (*Wydawanie dowodu osobistego*), data zgłoszenia: 2 marca 2015 r., data rozwiązania: 19 maja 2015 r., data zamknięcia zgłoszenia: 19 maja 2015 r. – obniżona dostępność usługi uwzględniona jedynie w raporcie za maj 2015 r.; **3)** Zgłoszenie 113502 (*Akceptacja wniosku o wydanie dowodu osobistego*), data zgłoszenia: 17 kwietnia 2015 r., data rozwiązania: 8 maja 2015 r., data zamknięcia zgłoszenia: 18 maja 2015 r. – obniżona dostępność usługi uwzględniona jedynie w raporcie za maj 2015 r.; **4)** Zgłoszenie 103014 (*Personalizacja blankietów*), data zgłoszenia: 16 marca 2015 r., data rozwiązania: 11 maja 2015 r., data zamknięcia zgłoszenia: 11 maja 2015 r. – obniżona dostępność usługi uwzględniona jedynie w raportach za kwiecień i maj 2015 r.; **5)** Zgłoszenie 93856 (*Przyjmowanie dowodu osobistego*), data zgłoszenia: 2 marca 2015 r., data rozwiązania: 11 maja 2015 r., data zamknięcia zgłoszenia: 11 maja 2015 r. – obniżona dostępność usługi uwzględniona jedynie w raporcie za maj 2015 r.

Organizacja wsparcia technicznego dla SRP

W strukturze organizacyjnej COI, w Pionie Eksploatacji Systemów funkcjonował Zespół Service Desk, który odpowiadał za wsparcie techniczne dla wszystkich systemów informatycznych utrzymywanych przez COI[51]. Wsparcie Zespołu Service Desk dla SRP realizowane było od czerwca 2014 r. W Service Desk COI pracowało 25 osób posiadających wiedzę i doświadczenie umożliwiające obsługę zgłoszeń dotyczących SRP, z tego 14 osób bezpośrednio obsługiwało zgłoszenia użytkowników SRP. Przed produkcyjnym uruchomieniem SRP, tj. przed 1 marca 2015 r., 12 pracowników świadczyło wsparcie dla przyszłych użytkowników SRP. Wsparcie obejmowało szkolenia, obsługę testów zewnętrznych i konfigurowanie stacji roboczych, przeglądarek i czytników, a także wsparcie dla Lokalnych Administratorów Ról w procesie nadawania uprawnień użytkownikom systemu.

Do zgłaszania problemów w działaniu SRP, COI udostępnił użytkownikom końcowym SRP System ITSM[52] pod nazwą *Atmosfera*. System ten umożliwia zarządzanie zgłoszonymi przez użytkowników problemami (incydentami) 24 godziny przez 7 dni w tygodniu[53] poprzez stronę internetową[54]. Dodatkowo dla dokonywania zgłoszeń udostępniona została linia telefoniczna oraz adres mailowy – obsługiwane również przez zespół konsultantów COI. Wpływające zgłoszenia o problemach (incydentach) są obsługiwane przez pracowników Zespołu Service Desk od poniedziałku do piątku w godz. 7–19 (administratorzy SRP są dostępni od poniedziałku do piątku w godz. 8–16). W przypadku zgłoszenia, które wpłynie poza standardowymi godzinami pracy Zespołu Service Desk jest ono obsługiwane od następnego dnia roboczego. W przypadku awarii krytycznej (gdy system jest niedostępny) administratorzy pracują nad rozwiązaniem problemu całą dobę, również w dni wolne od pracy.

Wsparcie techniczne SRP świadczone było w COI w oparciu o trzy linie wsparcia. I tak:

- pracownicy pierwszej linii wsparcia w Zespole Service Desk odpowiadali za rejestrowanie, kategoryzację i priorytetyzację incydentów, świadczenie wsparcia w ramach I linii dla użytkowników, analizowanie i rozwiązywanie incydentów, monitorowanie całego cyklu obsługi incydentu, a także dokumentowanie informacji, aktywności oraz rozwiązań. W przypadku gdy pracownik pierwszej linii wsparcia nie posiadał odpowiednich kompetencji do obsługi zgłoszenia, przekazywał je do drugiej linii wsparcia. W ramach pierwszej linii wsparcia w COI zgłoszenia obsługiwało 10 osób;
- drugą linię wsparcia tworzył zespół analityczno-merytoryczny Service Desk oraz pozostałe zespoły IT w COI. Wydzielone były tzw. zespoły wsparcia, składające się z pracowników COI (czasem z różnych komórek organizacyjnych). Zgodnie z załącznikiem nr 1 do *instrukcji obsługi incydentu pl.ID*, specjalista drugiej linii wsparcia odpowiadał za analizowanie, rozwiązywanie incydentów przekazanych przez pierwszą linię wsparcia, jeżeli nie posiadał odpowiednich kompetencji do obsługi zgłoszenia przekazywał je do trzeciej linii wsparcia (tzw. eskalowanie obsługi incydentów);

[51] M.in. SRP, Centralnej Ewidencji Pojazdów i Kierowców, elektronicznej Platformy Usług Administracji Publicznej, systemu do zarządzania dokumentami – eDOC, Centralnej Ewidencji Wydanych i Unieważnionych Dokumentów Paszportowych, Publikatora Aktów Prawnych i innych mniejszych systemów.

[52] Ang. IT Services Management – zarządzanie usługami IT.

[53] Za wyjątkiem krótkich przerw serwisowych.

[54] https://pomoc.coi.gov.pl

- trzecią linię wsparcia w ramach infrastruktury SRP stanowili zewnętrzni dostawcy elementów infrastruktury lub oprogramowania, którzy na podstawie umów gwarancyjnych lub pogwarancyjnych zawartych z COI, świadczyli usługi wsparcia w zakresie sprzętu i oprogramowania. W zakresie aplikacji trzecią linię wsparcia realizował Pion Rozwoju Systemów COI.

Wsparcie techniczne dla użytkowników SRP zostało zorganizowane zgodnie ze współczesną praktyką w tym zakresie.

Obsługa zgłoszeń użytkowników o problemach w funkcjonowaniu SRP, zarejestrowanych w systemie ITSM Atmosfera

W okresie od 1 marca 2015 r. do 15 czerwca 2016 r. użytkownicy SRP zgłosili łącznie 40 197 incydentów. Analiza wykazała, że 96,3% zgłoszonych problemów (tj. 38 721) zostało rozwiązanych. Natomiast w przypadku 369 zgłoszeń ich realizacja została czasowo wstrzymana i oczekiwała na wznowienie, a 1 106 incydentów posiadało status „Otwarte", tj. były rozwiązywane.

Analiza rozwiązanych problemów (incydentów) zarejestrowanych przez Service Desk COI w ww. okresie wykazała, że 23,6% incydentów rozwiązano w ciągu godziny od jego zgłoszenia; 14,1% – w ciągu doby; 14,7% – do tygodnia; 23,3% – do miesiąca, a 15% – do trzech miesięcy. Należy przy tym wskazać, że na rozwiązanie 9,3% incydentów Service Desk COI potrzebował do roku czasu.

Według stanu na dzień 15 czerwca 2016 r., na rozwiązanie oczekiwało 1 106 zgłoszeń problemów o statusie „Otwarte", z tego: 0,5% zgłoszono do 24 godzin, 3,2% do tygodnia, 8,7% do miesiąca, 22,1% do trzech miesięcy, 59,9% do roku czasu, a 5,7% zgłoszeń problemów pozostawało nie załatwionych przez COI od ponad roku. Analiza ww. 1 106 zgłoszeń pozostających jako otwarte wykazała, że 703 zgłoszenia miały charakter incydentalny (63,6%), a pozostałe 403 były powtarzalne.

Z informacji uzyskanych w COI wynika, że utrudnieniem w sprawnym rozwiązywaniu części zgłoszonych problemów była komunikacja z Ministerstwem (dawniej MSW, obecnie MC), gdyż czas odpowiedzi na pytania skierowane do Ministerstwa rzadko był krótszy niż dwa miesiące, a ponadto odpowiedzi czasem były ogólnikowe.

Zapewnione przez COI wsparcie techniczne SRP umożliwiało rozwiązywanie problemów, ale terminy ich rozwiązywania, zwłaszcza w pierwszych miesiącach po uruchomieniu systemu, były zbyt długie. Przez pierwsze 9 miesięcy rozwiązanie ponad 43% zgłoszeń zajmowało przynajmniej 1 miesiąc (w pierwszym miesiącu działania dotyczyło to aż 56% zgłoszeń). Oznacza to, że zgłoszenia nie były obsługiwane na bieżąco, a użytkownicy doświadczali utrudnień w realizacji ich bieżących zadań. Efektywność wparcia technicznego SRP ulegała stopniowej poprawie, lecz dopiero w czerwcu 2016 r. wsparcie techniczne zaczęło funkcjonować skutecznie. Świadczy o tym fakt, że 83,6% incydentów rozwiązywano w ciągu jednego dnia, w tym 60,8% z nich rozwiązywano już w ciągu godziny, a pozostałe 22,8% w ciągu doby. Przyczyną dużej liczby zgłoszeń w początkowym okresie eksploatacji było przedwczesne uruchomienie SRP. System nie był wówczas wystarczająco przetestowany, ani nie posiadał wszystkich wymaganych funkcjonalności, w szczególności w zakresie modułu BUSC i aplikacji „Źródło". W efekcie pierwsza linia wsparcia nie znając rozwiązania problemu nie mogła skutecznie udzielić pomocy użytkownikom (czyli nie spełniała funkcji zapory przed nadmierną liczbą zgłoszeń kierowanych do kolejnych linii), a niezbędne było często działanie drugiej, a niekiedy też trzeciej linii wparcia. Te zaś uległy przeciążeniu wskutek realizacji zbyt dużej liczby zgłoszeń. Jednocześnie wiele

zgłoszeń nie mogło zostać rozwiązanych, gdyż wymagały podjęcia decyzji o dokonaniu istotnych zmian w systemie, a zaznaczyć należy, że pierwsza linia wsparcia nie dysponuje możliwością skorygowania działania systemu, czy usunięcia usterki – może jedynie poinstruować użytkowników odnośnie właściwego sposobu postępowania w danych okolicznościach. Istotny w tym zakresie był też brak przez pierwszy rok eksploatacji umowy rozwojowej SRP pomiędzy COI a MSW/MC, która pozwoliłaby na rozwiązanie wielu problemów. Na sprawność wsparcia technicznego wpływ miał także długi czas korespondencji z właścicielem systemu (najpierw MSW, a potem MC).

Zarządzanie zmianami oprogramowania SRP

Analiza zmian w SRP dokonanych w okresie od lutego 2015 r. do sierpnia 2016 r. wykazała, że większość wprowadzanych modyfikacji miała na celu usunięcie usterek, które ujawniły się po uruchomieniu SRP. Usterki te dotyczyły różnego typu błędów w funkcjonalnościach SRP, jak np. błędnego zapisu danych, błędów w raportach, czy błędnego zachowania aplikacji „Źródło". W innych przypadkach modyfikacje zmierzały do poprawy wydajności systemu, np. w zakresie funkcji unieważniania dowodu. Inne modyfikacje dotyczyły wprowadzenia nowych funkcjonalności lub rozszerzenia funkcjonalności już istniejących i miały miejsce pod koniec wskazanego powyżej okresu. **Powyższe wskazuje, że jakość systemu w chwili uruchomienia nie była zadowalająca.**

Wyniki kontroli wykazały, że środowiska testowe SRP służące do badania, weryfikowania projektowanych zmian są adekwatne pod względem konfiguracji ich oprogramowania do środowiska rzeczywistego. **W ocenie NIK, zmiany w oprogramowaniu SRP były odpowiednio testowane, na środowisku testowym o odpowiednich parametrach.**

Szkolenia dla użytkowników SRP

We wszystkich kontrolowanych urzędach (13) zapewniono szkolenia związane z SRP dla pracowników obsługujących sprawy z zakresu dowodów osobistych, meldunków lub aktów stanu cywilnego.

Bezpłatne szkolenia dla użytkowników końcowych programu *pl.ID* były prowadzone według modelu hybrydowego, polegającego na połączeniu jednodniowych, stacjonarnych warsztatów bezpośrednich dla liderów z gmin i USC (po jednej osobie z każdej jednostki) z indywidualnymi szkoleniami online dla wszystkich użytkowników[55].

W okresie od 1 lipca 2014 r. do 27 listopada 2014 r. COI prowadził szkolenia stacjonarne dla tzw. liderów. Składały się z części teoretycznej (obejmującej m.in. cele programu *pl.ID*, zasady funkcjonowania SRP, najważniejsze zmiany prawne oraz zasady bezpieczeństwa przetwarzania danych) oraz z ćwiczeń praktycznych polegających na wykonywaniu wybranych czynności związanych z praktycznym wykorzystaniem szkoleniowej wersji SRP. W szkoleniach dla liderów wzięło udział 4 167 urzędników. Szkolenia z zakresu PESEL i RDO zostały ocenione dobrze przez 90% uczestników, natomiast szkolenia z BUSC dobrze oceniło 64% szkolonych, a 21% osób podało odpowiedź „trudno powiedzieć". Większość uczestników szkoleń pozytywnie oceniła aplikację „Źródło"[56].

[55] Dla przedstawicieli MSW, Centrum Personalizacji Dokumentów, Agencji Bezpieczeństwa Wewnętrznego, Poltransplantu (użytkownika Centralnego Rejestru Sprzeciwów), Kancelarii Prezydenta RP (użytkownika Systemu Odznaczeń Państwowych) COI przeprowadził szkolenia dedykowane. Łącznie w szkoleniach dedykowanych uczestniczyło 170 osób.

[56] Obszar: „podpowiedzi aplikacji" pozytywnie oceniło 70% respondentów, „wygląd" – 70% respondentów, „szybkość znajdowania funkcjonalności" – 66% respondentów, „łatwość orientacji oraz obsługi" – 67%.

W okresie od 13 sierpnia 2014 r. do 25 marca 2015 r. COI udostępnił użytkownikom końcowym możliwość szkolenia w formie e-learningu[57]. Użytkownicy mieli dostęp m.in. do filmów instruktażowych, podręczników szkoleniowych, zestawów ćwiczeń i testów samosprawdzających. Z tej formy szkolenia skorzystało 11 625 użytkowników[58]. Szkolenia z zakresu działania: modułu RDO pozytywnie oceniło 78% szkolonych, modułu PESEL – 82% uczestników szkoleń, natomiast z zakresu działania modułu BUSC – pozytywnie oceniło tylko 58% biorących udział w szkoleniu, 19% osób uczestniczących w szkoleniu z modułu BUSC stwierdziło, że zasady działania tego modułu są niezrozumiałe, a kolejne 23% szkolonych nie miało zdania na ten temat.

Użytkownikom SRP została udostępniona także szkoleniowa wersja aplikacji „Źródło"[59], w której na dzień 30 grudnia 2014 r. zarejestrowało się 8 187 użytkowników[60].

W dniach 10–12 grudnia 2014 r. oraz 19–23 stycznia 2015 r. COI zorganizował dla użytkowników SRP egzamin ze znajomości obsługi systemu. Polegał on na wykonaniu w aplikacji szkoleniowej „Źródło" zadań praktycznych z zakresu modułów PESEL, RDO lub BUSC (do wyboru w zależności od obszaru w jakim urzędnik wykonuje swoje obowiązki służbowe). Egzamin zaliczyło 10 025 użytkowników SRP, przy czym jedna osoba mogła zdawać od jednego do trzech egzaminów, tj. dla każdego modułu odrębnie. Łączna liczba wszystkich zdanych egzaminów wyniosła 19 327[61].

Za realizację całego procesu szkoleń w ramach zlecenia nr 24/PLID/2013 COI otrzymał wynagrodzenie w wysokości 3 510,9 tys. zł brutto.

Po wdrożeniu SRP COI zorganizował odpłatne szkolenia dla użytkowników końcowych SRP z jednostek samorządu terytorialnego. Dyrektor COI poinformował, że decyzja o prowadzeniu takich szkoleń wynikała z faktu, że *po uruchomieniu SRP 1 marca 2015 r. COI otrzymywał wiele sygnałów z gmin, że istnieje potrzeba dodatkowych szkoleń obsługi aplikacji, a jednocześnie ustalono, że w zakresie możliwości finansowych projektu ani budżetu MSW nie leżała wówczas możliwość zlecenia tych prac COI przez MSW.*

Odpłatność za przeszkolenie jednego użytkownika SRP wynosiła 400 zł. W trakcie 53 szkoleń zostało przeszkolonych 802 pracowników jednostek samorządu terytorialnego.

Na podstawie kolejnej umowy na utrzymanie SRP nr 2/DIT/U/COI/2016 zawartej w dniu 30 czerwca 2016 r. pomiędzy MC a COI, COI zostało powierzone zadanie realizacji szkoleń, w tym m.in. przygotowywanie scenariuszy filmów szkoleniowych dla użytkowników aplikacji „Źródło", nagrywanie filmów szkoleniowych i zamieszczanie ich na kanale YouTube, prowadzenie szkoleń dla urzędników korzystających z aplikacji „Źródło" w miejscu ich pracy oraz prowadzenie warsztatów szkoleniowych dla urzędników zgodnie z zapotrzebowaniem zgłaszanym przez poszczególne jednostki.

Szkolenia były zorganizowane w sposób umożliwiający przygotowanie użytkowników do pracy w SRP.

[57] https://szkolenia.obywatel.gov.pl

[58] Według *Raportu końcowego z realizacji zlecenia nr 24/PLID/2013* z 21 kwietnia 2015 r.

[59] https://szkolenia-zrodlo.obywatel.gov.pl

[60] Według *Raportu końcowego z realizacji zlecenia nr 24/PLID/2013* z 21 kwietnia 2015 r.

[61] Egzamin z modułu PESEL zdało 7 100 użytkowników, z modułu RDO – 6 745 użytkowników, z modułu BUSC – 5 482 użytkowników.

3.3 Zapewnienie bezpieczeństwa SRP i jego danych

3.3.1. Zarządzanie bezpieczeństwem SRP

Polityka bezpieczeństwa

COI stanowił pierwszą linię w zarządzaniu bezpieczeństwem SRP, realizując podstawowe procedury reagowania na incydenty bezpieczeństwa, natomiast bardziej zaawansowane działania, będące reakcją na te incydenty realizował, MC we współpracy z CERT[62] i Agencją Bezpieczeństwa Wewnętrznego.

Zadania COI w zakresie zarządzania bezpieczeństwem SRP określone zostały w umowach z MSW/MSWiA/MC na utrzymanie SRP. Zakres zadań powierzonych COI obejmował m.in. monitorowanie bezpieczeństwa systemu, zapewnienie bezpieczeństwa zmian oraz zarządzanie incydentami bezpieczeństwa. **COI należycie wywiązywał się z powierzonych mu zadań w zakresie bezpieczeństwa SRP**.

Zarządzanie bezpieczeństwem systemu SRP realizowane było w oparciu o *Politykę Bezpieczeństwa rejestrów państwowych w MSW objętych projektem pl.ID*[63], opracowaną przez Departament Teleinformatyki MSW (dalej: *Polityka Bezpieczeństwa pl.ID*). Celem wprowadzonej *Polityki Bezpieczeństwa pl.ID* było zapewnienie integralności, poufności, rozliczalności, niezaprzeczalności i niezawodności zasobów wchodzących w skład środowiska *pl.ID* oraz zagwarantowanie stałej dostępności świadczonych usług, a w szczególności zapewnienie wymaganego poziomu bezpieczeństwa i niezawodności przetwarzania informacji niezbędnych do sprawnej realizacji zadań z zakresu rejestrów państwowych.

Minister Cyfryzacji podała, że *w związku z trwającymi procesami restrukturyzacyjnymi w ramach MC* ***nie przeprowadzano analizy ryzyka w zakresie bezpieczeństwa informacji SRP.*** Według stanu na 7 września 2016 r. prowadzone były wstępne prace analityczne w tym zakresie.

Według NIK, *Polityka Bezpieczeństwa pl.ID*, będąca jedną z podstaw zarządzania bezpieczeństwem SRP, w tym w COI, w większości obszarów zawiera jedynie cel oraz krótkie przedstawienie danego zagadnienia. Brakuje w niej szczegółowych informacji zawierających odpowiednie procedury związane z tymi obszarami, nie opracowano także konkretnych dokumentów, do których odsyła *Polityka Bezpieczeństwa pl.ID*. W szczególności, w *Polityce Bezpieczeństwa pl.ID* brakuje zdefiniowanych procedur: komunikacji między COI a ministerstwem pełniącym funkcje zarządcze w zakresie SRP, zarządzania kontami użytkowników[64], nadawania i administrowania uprawnieniami; brakuje w pełni zdefiniowanej polityki zarządzania kontrolą dostępu do SRP, polityki bezpieczeństwa osobowego oraz systemu zarządzania ciągłością działania. W pkt. 6 *Polityki Bezpieczeństwa pl.ID* podano, że zasady funkcjonowania Systemu Zarządzania Bezpieczeństwem Informacji określają odrębne dokumenty. Z informacji przekazanych przez Minister Cyfryzacji wynika, że powyższe dokumenty nie powstały z *Polityką Bezpieczeństwa pl.ID*. Ponadto, Minister Cyfryzacji poinformowała, że *dokumenty określające zasady funkcjonowania*

---

62 Rządowy Zespół Reagowania na Incydenty Komputerowe.

63 Dokument z dnia 24 lutego 2015 r.

64 Zarządzanie kontami użytkowników zostało opisane w *Podręczniku Administratora Aplikacji Źródło*, *Dokumentacji Użytkownika Aplikacji Źródło – Podręcznik dla MSW* oraz w *Podręczniku Administratora Aplikacji Źródło – Administrator Lokalny*, jednakże wymienione podręczniki nie stanowią dokumentacji procesu zarządzania kontami użytkowników. Są to instrukcje użytkownika dla administratorów systemu Źródło.

Systemu Zarządzania Bezpieczeństwem (SZBI) nie powstały jeszcze w MC. (…) prowadzone są prace związane z kształtem i treścią SZBI. (…) w przygotowaniu jest natomiast aktualizacja samej Polityki Bezpieczeństwa.

COI przyjęło do realizacji zadania w zakresie zarządzania bezpieczeństwem SRP w sytuacji gdy system zarządzania bezpieczeństwem informacji nie został precyzyjnie zdefiniowany przez właściciela systemu.

Poza *Polityką Bezpieczeństwa pl.ID* ustanowioną przez MSW, COI realizował zarządzanie bezpieczeństwem SRP na podstawie *Polityki Bezpieczeństwa Informacji Centralnego Ośrodka Informatyki*, wprowadzonej zarządzeniem Nr 63/2015 Dyrektora COI z dnia 26 października 2015 r. Integralną częścią tej *Polityki* była m.in. procedura zgłaszania incydentu bezpieczeństwa. Dyrektor COI poinformował, że *polityka jest sukcesywnie wdrażana. Trwają prace przygotowawcze związane z wdrożeniem w organizacji normy ISO 27001, w ramach której zostanie dokonana analiza (kontrola) istniejącego systemu bezpieczeństwa informacji. Harmonogram działań związanych z wdrożeniem ISO 27001 jest w trakcie ustalania*.

Zarządzanie incydentami bezpieczeństwa

W okresie od 1 marca 2015 r. do 15 czerwca 2016 r. COI odnotował 142 zgłoszenia podejrzenia incydentów bezpieczeństwa. Część potwierdzonych incydentów bezpieczeństwa dotyczyła podłączenia stacji komputerowej wykorzystującej aplikację „Źródło" do publicznej sieci Internet. Minister Cyfryzacji podała, że na ww. stacjach *nie jest dozwolona konfiguracja sieciowa umożliwiająca nawiązywanie połączeń wychodzących do sieci Internet. Zalecana jest pełna separacja stacji dostępowych do SRP od innych sieci*. Dyrektor Pionu Bezpieczeństwa COI wyjaśnił, że *wszystkie incydenty z zakresu bezpieczeństwa są sygnalizowane MC, w sposób zgodny z Polityką Bezpieczeństwa pl.ID*.

Kierownik Zespołu Administratorów Systemów z COI potwierdził, że *zdarzało się, że komputer korzystając z systemu był jednocześnie podłączony do Internetu. Jest to poza gestią zarówno COI, jak i MC, można tylko poinformować gminę o zakazie.* Minister Cyfryzacji poinformowała, że *decyzję o wyciągnięciu ewentualnych konsekwencji za naruszenie ww. zasad podejmuje Departament Teleinformatyki MSWiA odpowiedzialny za infrastrukturę sieciową OST 112. (…) w praktyce każdorazowe zdiagnozowane naruszenie ww. zasad jest przekazywane do administratorów sieci MSWiA.* Podsekretarz Stanu w MSWiA poinformował natomiast, że *MSWiA nie dysponuje narzędziami określonymi przez obowiązujące przepisy prawne, pozwalającymi na wyciąganie (…) konsekwencji wobec gmin. W związku z tym, MSWiA skierowało do Ministerstwa Cyfryzacji w dniach 6 kwietnia i 26 sierpnia 2016 r. pisma z prośbą o podjęcie stosownych działań w zakresie uregulowań prawnych i polityki bezpieczeństwa SRP*.

Ponadto, Kierownik Zespołu Produkcji Oprogramowania II w COI poinformował, że *z inicjatywy COI opracowano narzędzie służące do sprawdzania czy stacja jest podłączona do sieci publicznej.* Dyrektor COI wskazał, że *narzędzie zostało uruchomione pilotażowo na okres tygodnia: 22–29.04.2016, żeby zweryfikować poprawność jego działania w środowisku produkcyjnym.*

Obsada zespołu zajmującego się bezpieczeństwem IT w COI była wystarczająca do zarządzania bezpieczeństwem SRP. COI podejmował działania w celu sprawnego zarządzania incydentami bezpieczeństwa, m.in. poprzez opracowanie narzędzia informującego o dostępie stacji roboczej z aplikacją „Źródło" do publicznej sieci Internet.

Zapewnienie rozliczalności działań podejmowanych przez użytkowników SRP

Wszystkie operacje wykonywane w SRP są zapisywane przez opracowany przez COI podsystem „Audyt". Funkcjonują następujące rejestry służące do audytu systemu:

- rejestr udostępnień, który przechowuje informacje o wszystkich wchodzących do systemu żądaniach udostępnienia danych. Zawiera takie informacje jak: podmiot żądający dostępu, wszystkie parametry żądania, datę i czas żądania, czy dane i w jakim zakresie zostały udostępnione. W dokumencie *Architektura Systemu Rejestrów Państwowych* wskazano, że rejestr udostępnień jest przystosowany do odnotowywania informacji wskazanych w § 7 ust. 1 pkt 4 rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych[65];
- rejestr zmian, który przechowuje informacje o tym jakie informacje zostały zmodyfikowane. Zawiera informacje takie jak: podmiot zmieniający dane, przedmiot zmiany, rodzaj zmiany, dane definiujące zmianę, datę i czas zmiany, czas realizacji żądania;
- rejestr podpisów (funkcjonuje podobnie do rejestru zmian).

W ocenie NIK, zapewniono odpowiednie mechanizmy kontrolne w ramach SRP, pozwalające na stwierdzenie kiedy i do jakich danych użytkownik uzyskał dostęp.

Zarządzanie uprawnieniami pracowników COI do pracy w SRP

Procedura nadawania i odbierania uprawnień do aplikacji „Źródło" dla pracowników COI polegała na przesłaniu przez wnioskującego stosownego wniosku według wzoru opublikowanego na stronie MC[66]. W przypadku dostępu do bazy danych, wnioskowanie odbywało się w trybie wniosku o zmianę. Proces ten opisano w *Instrukcji Zarządzania Zmianą SRP wraz z Komponentami powiązanymi, CEWiUDP*[67]*, PIA*[68] oraz *Instrukcji Zarządzania Zmianą ZIR*[69], uzgodnionych przez COI i MC.

Badanie przeprowadzone na próbie 10 pracowników COI wykonujących zadania w SRP wykazało, że zgodnie z § 20 ust. 2 pkt 4 rozporządzenia KRI, osoby te uczestniczyły w procesie przetwarzania informacji w stopniu adekwatnym do zadań wynikających z ich zakresów obowiązków. Ponadto ustalono, że dwie osoby posiadały konta dostępu do bazy danych w SRP pomimo zakończenia zatrudnienia w COI[70]. Było to niezgodne z § 20 ust. 2 pkt 5 rozporządzenia KRI, stanowiącym że zarządzanie bezpieczeństwem informacji realizowane jest w szczególności poprzez bezzwłoczną zmianę uprawnień w przypadku zmiany zadań osób zaangażowanych w proces przetwarzania informacji, a także z pkt A.9.2.6. załącznika A normy PN-ISO/IEC 27001:2014-12, stanowiącym, że przydzielone pracownikom prawa dostępu do informacji i środków przetwarzania informacji należy odbierać po zakończeniu zatrudnienia.

Powyższe było niezgodne także z pkt 9.5 tiret 7 *Polityki Bezpieczeństwa Informacji Centralnego Ośrodka Informatyki*, stanowiącej że prawa dostępu pracowników oraz osób/podmiotów świadczących usługi na rzecz COI po zakończeniu zatrudnienia lub obowiązywania właściwej

65 Dz. U. Nr 100, poz. 1024.

66 https://mc.gov.pl/wnioski-o-dostep-do-systemu-rejestrow-panstwowych

67 Centralna Ewidencja Wydanych i Unieważnionych Dokumentów Paszportowych.

68 Portal Informacyjny Administracji.

69 Zintegrowana Infrastruktura Rejestrów.

70 Zakończenie zatrudnienia nastąpiło odpowiednio z dniem 31 października 2015 r. i 31 maja 2016 r.

umowy są odbierane lub dostosowywane do zaistniałych zmian. Ponadto, w pkt 2.4 procedury nr PB008 „Zasady nadawania, usuwania i modyfikacji uprawnień", będącej uzupełnieniem ww. Polityki Bezpieczeństwa COI, podano, że w przypadku gdy zachodzi konieczność usunięcia, bądź modyfikacji nadanych użytkownikowi uprawnień wniosek o usunięcie/modyfikację uprawnień składa kierownik komórki organizacyjnej użytkownika do administratora systemu.

W trakcie kontroli ww. konta zostały zablokowane 14 lipca 2016 r., tj. odpowiednio po 257 i 44 dniach od zakończenia przez pracowników zatrudnienia.

Dyrektor COI wyjaśnił, że konta nie zostały zablokowane *w związku z zakłóceniami w przepływie informacji dotyczących ruchów kadrowych w COI. (...) Pragniemy podkreślić, że pomimo niezablokowanego konta, użytkownik nie mógł zalogować się do bazy ze względu na brak fizycznego dostępu. Dostęp jest możliwy tylko w wydzielonej strefie, z wydzielonej stacji roboczej i tyko z wydzielonej sieci. Aby dostać się do wydzielonych pomieszczeń użytkownik musi być pracownikiem COI i/lub posiadać kartę umożliwiającą dostęp do wydzielonych pomieszczeń. Karty takie są oddawane przez pracowników rozwiązujących umowę o pracę w ramach procesu rozliczania się z pracodawcą. W przypadku przebywania w strefie jako „gość" dostęp jest możliwy tylko w asyście pracownika COI.* Dyrektor COI poinformował, że nie odnotowano logowania na opisanych kontach byłych pracowników po zakończeniu przez nich zatrudnienia.

Audyty i testy bezpieczeństwa SRP

W trakcie wytwarzania SRP były przeprowadzone[71] przez podmioty zewnętrzne, audyty i testy bezpieczeństwa systemu. Audytem objęto jakość kodu źródłowego i odporność systemu na ataki z zewnątrz. W przypadku stwierdzenia podatności systemu wdrożono odpowiednie poprawki oraz przeprowadzono powtórne audyty i testy bezpieczeństwa.

Audyty i testy bezpieczeństwa przeprowadzane były jedynie w trakcie wytwarzania i wdrażania SRP i od chwili jego uruchomienia (czyli prawie półtora roku), pomimo wprowadzenia licznych zmian w systemie, nie został przeprowadzony żaden audyt/test bezpieczeństwa SRP. Dyrektor Pionu Bezpieczeństwa COI podał, że testy bezpieczeństwa SRP są planowane na III/IV kwartał 2016 r. oraz, że *trwają ustalenia z Ministerstwem Cyfryzacji co do terminu i zakresu testów bezpieczeństwa*.

3.3.2. Zapewnienie bezpieczeństwa informacji w kontrolowanych urzędach miast

Uregulowania wewnętrzne z zakresu bezpieczeństwa informacji

W ośmiu objętych kontrolą urzędach[72], tj. 62%, nie opracowano i nie wdrożono polityki bezpieczeństwa informacji, która jest elementem systemu zarządzania bezpieczeństwem informacji, wymaganym przez § 20 ust. 3 w związku z ust. 1 rozporządzenia KRI. W myśl tego przepisu wymagania w zakresie systemu zarządzania bezpieczeństwem informacji uznaje się za spełnione, jeżeli zostały opracowane na podstawie Polskiej Normy PN-ISO/IEC 27001 *Technika informatyczna. Techniki bezpieczeństwa. Systemy zarządzania bezpieczeństwem informacji. Wymagania* oraz powiązanej z nią Polskiej Normy PN-ISO/IEC 17799 *Technika informatyczna*.

[71] W okresie od lipca 2014 r. do stycznia 2015 r.

[72] Dotyczy to UM: Bielsk Podlaski, Krosno, Legionowo, Łomża, Piaseczno, Przemyśl, Rzeszów, Warszawa.

Techniki bezpieczeństwa. Praktyczne zasady zarządzania bezpieczeństwem informacji. W pkt 5.1 normy PN-ISO/IEC 17799 wskazano opracowanie i stosowanie dokumentu polityki bezpieczeństwa informacji.

Opracowane i wdrożone w kontrolowanych jednostkach regulacje nie obejmowały wszystkich informacji jakie są przetwarzane w urzędzie[73], lecz dotyczyły głównie danych osobowych. Kontrolowani wskazywali m.in., że planowane są, bądź zostały podjęte prace dla przygotowania nowej Polityki Bezpieczeństwa Informacji, która obejmie wszystkie elementy systemu zarządzania bezpieczeństwem informacji w urzędzie. Na przykład:

- W **Urzędzie Miasta Legionowo** w okresie objętym kontrolą obowiązywały zarządzenia[74] Prezydenta Miasta w sprawie wprowadzenia Polityk Bezpieczeństwa w Urzędzie Miasta, które nie obejmowały całościowo zagadnień określonych w rozporządzeniu KRI, a dotyczyły wyłącznie ochrony danych osobowych. Prezydent Miasta poinformował, iż opracowanie i wdrożenie Polityki Bezpieczeństwa Informacji jest w trakcie realizacji.
- W **Urzędzie m.st. Warszawy** nie opracowano dokumentu polityki bezpieczeństwa informacji. Sekretarz Miasta poinformował, że przedłożony w toku kontroli zestaw dokumentów w postaci zarządzeń, standardów oraz procedur reguluje obecnie sprawy związane z bezpieczeństwem informacji w Urzędzie m.st. Warszawy. Jak podał Sekretarz Miasta aktualizacja procedur i standardów następuje stosownie do potrzeb, oraz że *(…) kierownictwo Urzędu m.st. Warszawy widzi potrzebę usystematyzowania obszaru związanego z bezpieczeństwem informacji, dlatego też został powołany zespół ds. opracowania i wdrożenia Polityki Bezpieczeństwa Informacji. W skład zespołu wchodzą przedstawiciele biur, między innymi: Biura Informatyki i Przetwarzania Informacji, Biura Bezpieczeństwa i Zarządzania Kryzysowego oraz Biura Organizacji Urzędu. Obecnie rzeczony dokument jest na etapie opracowania i uzgadniania treści.* Prezydent Miasta poinformowała, iż ww. projekt jest uzgadniany pomiędzy wewnętrznymi komórkami Biura Organizacji, a następnie zostanie przekazany do uzgodnień do biur Urzędu m.st. Warszawy oraz Urzędów Dzielnic.

Pozostałe cztery urzędy[75] objęte badaniem (tj. 31%), opracowały i wdrożyły procedury regulujące politykę bezpieczeństwa informacji.

Zarządzanie uprawnieniami użytkowników aplikacji „Źródło"

W myśl § 20 ust. 2 pkt 4 i 5 rozporządzenia KRI, zarządzanie bezpieczeństwem informacji realizowane jest m.in. przez podejmowanie 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, a w przypadku zmiany zadań następuje również zmiana uprawnień.

W kontrolowanych urzędach stosowano wytyczne MSW[76] w zakresie nadawania, modyfikowania i odbierania uprawnień użytkownikom aplikacji „Źródło". Ponadto, w pięciu urzędach[77] opracowano i wdrożono pisemne procedury zarządzania uprawnieniami użytkowników w systemach informatycznych, w tym w aplikacji „Źródło".

73 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.

74 z dnia 6 listopada 2013 r. nr 192/2013 i z dnia 1 czerwca 2016 r. nr 115/2016.

75 UM: Otwock, Świdnica, Wałbrzych i Wrocław.

76 Pismo nr DEP-WAP-0460-63-2/2015 z dnia 26 października 2015 r. skierowane do wójtów, burmistrzów i prezydentów miast.

77 UM: Otwock, Piaseczno, Przemyśl, Wałbrzych, Warszawa.

Badanie przyznanych uprawnień dostępu do aplikacji „Źródło", dokonane na łącznej próbie 177 pracowników kontrolowanych urzędów, wykazało, że w przypadku ośmiu osób[78] (5%) nadane uprawnienia były nieadekwatne do zadań określonych w zakresach czynności tych osób. Na przykład:

- W **Urzędzie Miejskim w Łomży** dwóm pracownikom przypisano w aplikacji „Źródło" większą liczbę ról, niż wynikałoby to z zakresu wykonywanych obowiązków[79], a w zakresach czynności kolejnych sześciu pracowników nie wskazano, że pełnią oni funkcję LAR[80] (przypisaną w SRP), co było niezgodne z § 20 ust. 2 pkt 4 rozporządzenia KRI oraz z § 9 pkt 4 Zarządzenia Prezydenta Miasta Łomży z 4 marca 2013 r. w sprawie Kontroli Zarządczej w Mieście Łomża, zgodnie z którym zakresy obowiązków, uprawnień i odpowiedzialności osób zarządzających i pracowników Urzędu Miejskiego powinny zostać określone pisemnie, w sposób precyzyjny, adekwatny do wagi podejmowanych decyzji (...). Z wyjaśnień Sekretarz Miasta wynika, że: *Nadanie zbyt wielu ról dwóm pracownikom (...) nastąpiło z powodu niewystarczającej znajomości funkcji Systemu. (...) Role wszystkich pracowników korzystających z SRP zostaną pilnie zweryfikowane i dostosowane do stanu faktycznego. Nieujęcie w zakresach obowiązków pracowników przypisanej w SRP roli LAR nastąpiło przez przeoczenie. Brak ten zostanie w najbliższym czasie usunięty.*

Siedmiu pracownikom pięciu urzędów[81], którzy zakończyli pracę w urzędzie (co stanowiło 16% z badanej próby 43 pracowników) nie odebrano uprawnień do dostępu do aplikacji „Źródło" i ich konta pozostawały wciąż aktywne. Na przykład:

- W **Urzędzie Miejskim w Przemyślu** dwóm osobom (na 10 badanych) uprawnienia (role) w aplikacji „Źródło" odebrano dopiero po 120 i 54 dniach od zakończenia przez nich pracy z tą aplikacją. Było to niezgodne z § 20 ust. 2 pkt 5 rozporządzenia KRI, stanowiącym że zarządzanie bezpieczeństwem informacji realizowane jest w szczególności poprzez bezzwłoczną zmianę uprawnień w przypadku zmiany zadań osób zaangażowanych w proces przetwarzania informacji. Opóźnienie w przekazaniu wniosku o odebranie uprawnień, spowodowane było prośbą Kierownika USC o powstrzymanie się z wyrejestrowaniem, w związku z planowanym, dalszym zatrudnieniem użytkownika oraz długotrwałą procedurą ponownego uzyskiwania karty kryptograficznej.

W przypadku trzech urzędów[82], NIK zwróciła również uwagę na długotrwałe przekazywanie do ministra właściwego do spraw informatyzacji wniosków o trwałe usunięcie kont użytkowników z aplikacji „Źródło". Na przykład:

- W **Urzędzie Miejskim w Białymstoku**, w związku z zakończeniem zatrudnienia przez trzech pracowników Urzędu (użytkowników aplikacji „Źródło"), dopiero po 140, 397 i 462 dniach przekazano do Ministerstwa Cyfryzacji wnioski o usunięcie kont z SRP. Zastępca Kierownika USC wyjaśniła, że przyczyną późnego złożenia wniosków było przeoczenie, jak również brak ściśle określonego terminu na złożenie stosownego wniosku.

Ochrona przetwarzanych informacji w aplikacji „Źródło" przed nieuprawnionym dostępem

Badania wykorzystania i przechowywania przez pracowników kontrolowanych urzędów (użytkowników aplikacji „Źródło") 104 kart kryptograficznych służących do elektronicznego podpisywania dokumentów w tej aplikacji wykazało, że z wyjątkiem jednego urzędu[83], we wszystkich kontrolowanych urzędach karty były przechowywane w sposób uniemożliwiający dostęp osób postronnych. Nie stwierdzono przypadków aby na kartach tych były zapisane numery PIN oraz PUK umożliwiające podpisywanie dokumentów.

78 Dotyczy UM w Łomży.

79 Dotyczy to pracowników USC, którym nadano role pn. *Urzędnik ewidencji ludności*.

80 Lokalny Administrator Ról. Osoba odpowiedzialna w urzędzie za zarządzanie uprawnieniami użytkowników aplikacji „Źródło".

81 UM (w nawiasie liczba osób): Przemyśl (2), Łomża (1), Bielsk Podlaski (1), Świdnica (2), Wrocław (1).

82 UM: Białystok, Legionowo i Łomża.

83 Urząd Miasta Otwocka.

- W **Urzędzie Miasta Otwocka** karty kryptograficzne trzech pracowników USC przechowywano w szufladach szafek, które nie zostały wyposażone w zamki, co było niezgodne z *Wymaganiami i zaleceniami bezpieczeństwa dla podmiotów wnioskujących o dostęp do SRP poprzez aplikację „Źródło"*[84]. Tłumaczono to niedopatrzeniem. Nieprawidłowość ta została usunięta w trakcie kontroli NIK.

Z przeprowadzonych w trakcie kontroli oględzin w 13 kontrolowanych urzędach na łącznie 105 stanowiskach pracy pracowników realizujących zadania z wykorzystaniem aplikacji „Źródło" wynika, że:

- w jednym urzędzie monitory usytuowane były w sposób umożliwiający wgląd do danych przez osoby nieuprawnione.
  - W **Urzędzie Miejskim w Łomży** usytuowanie dwóch monitorów na stanowiskach pracy realizujących zadania w aplikacji „Źródło", umożliwiało wgląd do wyświetlanych na nich treści osobom postronnym, co naruszało § 20 ust. 2 pkt 9 rozporządzenia KRI, zgodnie z którym informacje powinny być zabezpieczone w sposób uniemożliwiający nieuprawnionemu jej ujawnienie oraz art. 36 ust. 1 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych[85], w myśl którego administrator danych jest obowiązany zastosować środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych. Sekretarz Miasta wyjaśniła, że wynikało to (…) *z warunków lokalowych. Monitory te są w oddaleniu od miejsca bezpośredniej obsługi interesantów uniemożliwiającym lub znacznie ograniczającym im możliwość odczytu danych. (…) W celu zapewnienia pełnej ochrony danych wyświetlanych na tych monitorach zostaną one zabezpieczone specjalną folią uniemożliwiającą odczyt danych z pozycji innej niż zajmowana przez pracownika bezpośrednio pracującego na stanowisku komputerowym*;
- w trzech urzędach[86] stacje komputerowe z aplikacją „Źródło" posiadały dostęp do Internetu. Było to niezgodne z *Wymaganiami dla stacji roboczych stanowisk obsługi dla użytkowników końcowych SRP*[87]. Na przykład:
  - W **Urzędzie m.st. Warszawy** stwierdzono, że komputery, na których wykorzystywana jest aplikacja „Źródło", mają dostęp do sieci Internet. Sekretarz Miasta poinformował, że *Wymóg fizycznej separacji stacji roboczych z systemem Źródło do sieci Internet kłóci się z logiką zapewnienia bezpieczeństwa tymże stacjom roboczym w aktualizacje systemu operacyjnego, aplikacji biurowych, oprogramowania JAVA, czy oprogramowania antywirusowego. Stosowanie polityk bezpieczeństwa stacji roboczych wynika z wewnętrznych regulacji Urzędu m.st. Warszawy, a w przypadku systemu „Źródło" z polityki bezpieczeństwa Systemu Rejestrów Państwowych. Problem ten jest permanentnie podnoszony przez administratorów informatycznych w gminach i skutecznie pomijany w rozmowach czy wytycznych przez COI i MC*. NIK zauważa, że w piśmie z dnia 16 grudnia 2014 r. MSW, udzielając odpowiedzi na pytania Urzędu m.in. w zakresie konfiguracji stanowisk komputerowych z aplikacją „Źródło", wyraźnie wskazało, że stanowiska nie mogą mieć możliwości bezpośredniego lub pośredniego ustanowienia sesji wychodzącej ani przesyłania informacji do sieci Internet. W odpowiedzi na wystąpienie pokontrolne Prezydent Miasta poinformowała, iż Miasto Stołeczne Warszawa wystąpi do Ministerstwa Cyfryzacji o dostosowanie wymogów proceduralnych związanych z architekturą IT tak, aby możliwe było zachowanie dostępu do sieci internetowej na stanowiskach, na których wykorzystywana jest aplikacja „Źródło".
  - W **Urzędzie Miejskim w Łomży** ustalono, że pięć stanowisk komputerowych mających dostęp do aplikacji „Źródło" posiadało dostęp do Internetu. W wyniku kontroli NIK, w dniu 24 czerwca 2016 r. odłączony został dostęp do Internetu na wszystkich komputerach z aplikacją „Źródło".

NIK zauważa, że z umożliwieniem dostępu do Internetu na stacjach komputerowych z aplikacją „Źródło" wiąże się ryzyko wycieku danych zgromadzonych w Systemie Rejestrów Państwowych. Za pomocą tej aplikacji przetwarzane są bowiem dane o obywatelach, w szczególności w zakresie aktów stanu cywilnego, dowodów osobistych, a także ewidencji PESEL. Zasady zabezpieczenia tak istotnych danych o obywatelach powinny być zatem

84 Wydane przez Ministerstwo Spraw Wewnętrznych i Centralny Ośrodek Informatyki obowiązujące od 1 marca 2015 r.

85 Dz. U. z 2016 r. poz. 922.

86 UM: Warszawa, Łomża, Otwock.

87 Wydane przez Ministerstwo Spraw Wewnętrznych i Centralny Ośrodek Informatyki.

bezwzględnie przestrzegane przez wszystkich użytkowników tego systemu. Zapewnieniu bezpieczeństwa danych w SRP służą wprowadzone przez COI wymagania w zakresie uniemożliwienia dostępu do Internetu na komputerach z aplikacją „Źródło". Należy zauważyć, że nie wypracowano w MC oraz MSWiA skutecznych rozwiązań pozwalających na egzekwowanie od kierowników urzędów stosowania się do zakazu podłączania stacji komputerowych z aplikacją „Źródło" do Internetu.

Audyt wewnętrzny z zakresu bezpieczeństwa informacji

W myśl § 20 ust. 2 pkt 14 rozporządzenia KRI, zarządzanie bezpieczeństwem informacji realizowane jest m.in. poprzez zapewnienie przez kierownictwo podmiotu publicznego warunków umożliwiających realizację i egzekwowanie działania polegającego na okresowym audycie wewnętrznym w zakresie bezpieczeństwa informacji, nie rzadziej niż raz na rok.

W **trzech urzędach**[88] (tj. 23%) w 2015 r. nie przeprowadzono audytu w zakresie bezpieczeństwa informacji w systemach informatycznych, co było niezgodne z § 20 ust. 2 pkt 14 rozporządzenia KRI.

W **10 jednostkach**, w których przeprowadzono coroczny audyt bezpieczeństwa informacji, sformułowane zalecenia, rekomendacje nie dotyczyły bezpośrednio SRP, jednak pośrednio oddziaływały na jego bezpieczeństwo, gdyż ukierunkowane były ogólnie na wzmocnienie bezpieczeństwa przetwarzania informacji.

Szkolenia pracowników z zakresu bezpieczeństwa informacji

Zgodnie z § 20 ust. 2 pkt 6 rozporządzenia KRI zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienie przez kierownictwo podmiotu publicznego warunków umożliwiających realizację i egzekwowanie szkolenia osób zaangażowanych w procesie przetwarzania informacji.

Za wyjątkiem jednego urzędu[89], we wszystkich pozostałych kontrolowanych urzędach, zorganizowano szkolenia dotyczące bezpieczeństwa informacji, w których brali udział użytkownicy aplikacji „Źródło". Tematyka szkoleń dotyczyła m.in. postępowania z informacją w urzędzie (w tym ochrony danych osobowych), bezpieczeństwa teleinformatycznego oraz ustanowionych w urzędach procedur w zakresie bezpieczeństwa informacji. Szkolenia prowadzone były zarówno przez pracowników urzędów, np. przez Administratora Bezpieczeństwa Informacji, jak i przez firmy zewnętrzne.

3.4 Wpływ uruchomienia SRP na funkcjonowanie wewnętrznych systemów informatycznych urzędów miast/miast i gmin wykorzystywanych do realizacji pozostałych spraw z zakresu obsługi obywatela

W kontrolowanych urzędach SRP współpracował bezpośrednio wyłącznie z aplikacjami odpowiedzialnymi za prowadzenie rejestru mieszkańców (ewidencji ludności). Zakres przekazywanych danych obejmował m.in.: imiona, nazwiska, nazwiska rodowe, numery PESEL, adresy zameldowania na pobyt stały i czasowy, stan cywilny, dane o współmałżonkach, dane

88 UM: Łomża, Otwock, Świdnica.

89 UM w Legionowie.

rodziców, miejsca urodzenia, serię i numer dowodu osobistego, datę zgonu. Dane przekazywane były za pomocą mechanizmu przyrostowej subskrypcji danych[90], w określonych odstępach czasu następowało pobieranie danych z SRP do gminnego rejestru mieszkańców, np.:

- W **Urzędzie Miasta Bielsk Podlaski** co 30 minut następowało automatyczne pobieranie danych z SRP do rejestru mieszkańców gminy prowadzonego w systemie ELUD+, z którego następnie dane przekazywane były do rejestru wyborców (WYB+). W Urzędzie wskazano, że *z informacji znajdującej się w systemie „Źródło" korzystają również inne referaty, jednak nie mają one bezpośredniego dostępu do tego systemu.*

Kontrolowani wskazywali na utrudnienia w sprawnej obsłudze obywateli w związku z brakiem możliwości bezpośredniego przekazywania do aplikacji „Źródło" danych zawartych w elektronicznych wnioskach (np. o wydanie dowodu osobistego) składanych za pośrednictwem platformy ePUAP. Na przykład:

- W **Urzędzie Miasta w Wałbrzychu** wniosek o wydanie dowodu osobistego złożony drogą elektroniczną przez ePUAP jest drukowany w wersji papierowej, załącznik w postaci zdjęcia zapisywany jest w katalogu sieciowym i jest dostępny dla określonych użytkowników. Pracownik realizujący zadanie przechodzi stanowisko komputerowe z aplikacją „Źródło" gdzie musi ręcznie wprowadzić wydrukowany wniosek i zaimportować zdjęcie. W przypadku niezgodności danych we wniosku albo niewłaściwego formatu załączonego zdjęcia, pracownik musi wrócić na stanowisko, na którym zaimportował wniosek aby poinformować obywatela o potrzebie korekty złożonego wniosku.

Uruchomienie SRP nie miało znaczącego wpływu na funkcjonowanie wewnętrznych systemów informatycznych wykorzystywanych w kontrolowanych urzędach. Zdaniem NIK, ułatwieniem w pracy urzędów byłoby umożliwienie bezpośredniej wymiany danych pomiędzy platformą ePUAP a SRP.

3.5 Wpływ udostępnienia SRP na koszt obsługi zadań w urzędach miast/miast i gmin

Po udostępnieniu SRP, w ponad połowie kontrolowanych urzędów (w siedmiu[91] spośród 13, tj. 54%) nastąpił wzrost zatrudnienia osób zajmujących się sprawami z zakresu stanu cywilnego, z czego największy nastąpił w Urzędzie m.st. Warszawy (z 142 do 190, tj. o 48 osób).

- Dyrektor **USC m.st. Warszawy** w październiku 2014 r. dokonała ilościowej analizy etatów potrzebnych do zapewnienia załatwiania spraw z zakresu rejestracji stanu cywilnego w związku z udostępnieniem SRP. W analizie wzięto pod uwagę m.in. nowe zadania pracowników USC, ilość dotychczas wydawanych odpisów, spraw oraz prognozę na 2015 r. W analizie zawarto propozycje rozwiązań, w tym m.in. zwiększenie zatrudnienia (min. o 30 pracowników), otwarcie nowej siedziby w jednej z dzielnic m.st. Warszawy. Ponadto, w 2015 r. Biuro Audytu Wewnętrznego Urzędu m.st. Warszawy przeprowadziło czynności doradcze pn. *„Efektywność obsługi ludności w Urzędzie Stanu Cywilnego w kontekście użytkowanej aplikacji Źródło, czyli Systemu Rejestrów Państwowych w świetle postanowień ustawy Prawo o aktach stanu cywilnego oraz Ustawy o ewidencji ludności"*. Audytorzy sformułowali rekomendacje mające na celu przyspieszanie migracji aktów stanu cywilnego poprzez zwiększenie zatrudnienia w archiwum o 10 osób, które będą migrować akty do SRP lub zwiększenie zatrudnienia w archiwum łącznie o 20 osób w systemie dwuzmianowym. Audytorzy wskazali, że przy przyjęciu pierwszego wariantu usprawnienia pracy, całkowite nadrobienie zaległości będzie możliwe we wrześniu 2020 r., natomiast przy przyjęciu drugiego wariantu we wrześniu 2017 r.

W pozostałych pięciu kontrolowanych urzędach[92] zatrudnienie nie zmieniło się w stosunku do stanu przed udostępnieniem SRP, a w jednym uległo zmniejszeniu[93].

---

90 Przekazywane są wyłącznie informacje o obywatelach, które zostały zmienione lub dodane, od czasu ostatniego pobrania danych.

91 UM (w nawiasie: wzrost liczby pracowników): Białystok (4), Krosno (1), Rzeszów (2), Świdnica (2), Wałbrzych (1), Warszawa (48), Wrocław (3).

92 UM: Bielsk Podlaski, Legionowo, Łomża, Otwock, Piaseczno.

93 UM w Przemyślu (spadek liczby pracowników o sześć osób).

W trzech kontrolowanych urzędach w związku z udostępnieniem SRP zlecano pracownikom wykonywanie dodatkowych prac w ramach godzin nadliczbowych lub umów cywilnoprawnych, tj.:

- W **Urzędzie Miasta i Gminy Piaseczno** wydatki na pracę w godzinach nadliczbowych wyniosły łącznie 23,2 tys. zł.
- W **Urzędzie Miejskim w Świdnicy** jednej osobie zlecano w ramach dwóch umów cywilnoprawnych wykonywanie dodatkowych prac. Przedmiotem tych prac była migracja aktów stanu cywilnego. W okresie od 1 czerwca 2015 r. do 30 czerwca 2016 r. za wykonanie tych prac poniesiono wydatki łącznie 27,2 tys. zł.
- W **Urzędzie m.st. Warszawy** pracownikom Biura Administracji i Spraw Obywatelskich zlecano wykonywanie pracy w godzinach nadliczbowych w celu poprawienia m.in. błędnego nazewnictwa ulic i numerów lokali, wyjaśniania rozbieżności danych między bazą lokalną. Wydatki na pracę w godzinach nadliczbowych w 2015 r. wyniosły łącznie 1 053,1 tys. zł. Dyrektor USC m.st. Warszawy wyjaśniła, że w okresie od 1 września 2015 r. do 30 kwietnia 2016 r. w godzinach nadliczbowych pracowało 12 pracowników. W ramach dodatkowych godzin pracownicy dokonywali migracji aktów stanu cywilnego, sporządzano akty urodzeń dzieci nowonarodzonych, nadawano numery PESEL dla noworodków, realizowano zlecenia migracji złożone w USC m.st. Warszawy oraz zlecenia innych USC w kraju oraz realizowano korespondencję z terenu Polski i z zagranicy. Wydatki na pracę w godzinach nadliczbowych w ww. okresie wyniosły łącznie 270,8 tys. zł.

Wraz z udostępnieniem aplikacji „Źródło" wzrosła liczba wydruków części dokumentów w zakresie aktów stanu cywilnego. Spowodowane to było wprowadzeniem z dniem 1 marca 2015 r. nowych dokumentów, których wcześniej nie było oraz zwiększoną liczbą stron niektórych dokumentów funkcjonujących już przed wprowadzeniem SRP. Dotyczyło to w szczególności takich dokumentów jak: uzupełnienie aktu małżeństwa, sprostowanie aktu małżeństwa, przyjęcie oświadczenia o uznaniu dziecka, przyjęcie zapewnienia o braku przeszkód do zawarcia związku małżeńskiego, zaświadczenie o braku przeciwwskazań do zawarcia związku małżeńskiego, protokół zgłoszenia urodzenia, powiadomienie o nadanym numerze PESEL.

Udostępnienie SRP bez przeprowadzenia wcześniejszej migracji aktów stanu cywilnego zgromadzonych w lokalnych systemach informatycznych wpłynęło na wzrost wydatków ponoszonych w niektórych kontrolowanych USC. W szczególności dotyczyło to wydatków związanych z zatrudnieniem dodatkowych pracowników oraz zlecania dodatkowych prac w ramach godzin nadliczbowych lub umów cywilnoprawnych.

3.6 Wpływ uruchomienia SRP na ograniczenie rozbieżności pomiędzy danymi zawartymi w poszczególnych rejestrach wchodzących w skład tego systemu

Przed 1 marca 2015 r. dane o obywatelach były gromadzone niezależnie od siebie w ogólnopolskim rejestrze PESEL oraz w ewidencji wydanych i unieważnionych dowodów osobistych. Księgi stanu cywilnego były prowadzone samodzielnie przez poszczególne gminy w postaci papierowej a w systemach informatycznych urzędów gromadzono dane niezbędne do wydruku aktu stanu cywilnego. Po 1 marca 2015 r. dane zgromadzone dotychczas w rejestrze PESEL oraz w ewidencji wydanych i unieważnionych dowodów osobistych zostały zintegrowane w jeden centralny System Rejestrów Państwowych. Rozpoczęła się także migracja danych w zakresie stanu cywilnego (co szerzej opisano w punkcie 3.2 Informacji).

3.6.1. Zapewnienie prawidłowości danych zgromadzonych w rejestrach SRP

W SRP wdrożono mechanizmy sprawdzania prawidłowości danych wprowadzanych do tego systemu (tzw. walidacja danych). Dane wprowadzane do SRP były w pierwszej kolejności weryfikowane na podstawie reguł walidacji. Dalszym poziomem weryfikacji danych były mechanizmy systemów zarządzania bazami danych, tzw. mechanizm kluczy obcych, określenie typów pól i mechanizm ograniczeń.

W kwestii zapewnienia spójności i poprawności danych w SRP, Kierownik Zespołu Produkcji Oprogramowania II z COI wyjaśnił, że *w toku prac nad migracją danych ujawniło się wiele błędów w danych. (…) Rezygnacja z walidacji konkretnych danych była uzgadniania z klientem (MSW). Pewne mechanizmy są cały czas aktywne.* Wskazał też, że *COI wnioskuje od dłuższego czasu o zlecenie w celu kompleksowej naprawy błędów w danych. O części błędów było informowane Ministerstwo Spraw Wewnętrznych i Ministerstwo Cyfryzacji. Istnieją w danych błędy biznesowe wynikające np. z braku standaryzacji kodów pocztowych. W danych historycznych można było mieć adres, który nie istnieje*.

Kierownik Zespołu Architektury i Standardów IT z COI wyjaśnił, że *były sytuacje, w których mechanizmy walidacji musiały zostać zdjęte z powodu niespójności danych historycznych. Takie decyzje były każdorazowo uzgadniane z MSW. W niektórych przypadkach nadawanie numerów PESEL odbywało się bez dostępu do systemu (Jantar). Numery sekwencyjne były wtedy celowo zawyżane (…), aby uniknąć konfliktów. Dokonano sprawdzenia i ustalono, że w systemie nie ma dwóch różnych osób o tym samym numerze PESEL (ograniczenie twarde w bazie danych) oraz niezgodności cyfry kontrolnej. Błędy typowe to – braki danych (np. nazwiska rodowego), literówki, błędy w danych słownikowych, błędy w numerach PESEL (część oparta na dacie nie pasuje do daty z kalendarza). Zdarza się, że bazy nie miały zachowanych więzów referencyjnych (np. dowód osobisty i osoba – dowody są przypisane do niewłaściwych osób). (…) Niektóre błędy uniemożliwiły migrację niektórych danych.*

Minister Cyfryzacji poinformowała, że obowiązujący przed wdrożeniem SRP trójstopniowy schemat zasilania ewidencji ludności skutkował bardzo często brakiem aktualizacji ówczesnego zbioru PESEL, gdyż wiele rekordów, pomimo przesłania aktualizacji z poziomu gminnego, nie trafiło do zbioru centralnego. Przyczyną były problemy techniczne, jak również zaniechania realizacji protokołów odrzutów na poziomie wojewódzkim. Świadomość niskiej jakości danych w zbiorze PESEL była jedną z ważniejszych przesłanek do wdrożenia SRP. Nastąpiła zmiana zasilania rejestrów centralnych i stopniowa poprawa ich jakości, w szczególności przez:

- aktualizację danych w czasie rzeczywistym;
- bezpośrednie przepływy rejestrowanych zdarzeń pomiędzy poszczególnymi komponentami SRP, co wyeliminowało konieczność ich ręcznego wprowadzania do poszczególnych rejestrów centralnych;
- wprowadzenie i ujednolicenie słowników dla poszczególnych danych gromadzonych w rejestrze PESEL – brak możliwości wprowadzania niejednolitego zapisu danych, np. nazw ulic, miejscowości.

Minister Cyfryzacji wśród działań zmierzających do poprawy jakości danych przed wdrożeniem SRP wymieniła m.in.:

- wybór ze zbioru PESEL oraz uzupełnienie we współpracy z organami gmin 11 300 rekordów w zakresie brakujących dat zgonu;
- uzupełnienie, we współpracy z organami gmin, ponad 100 000 rekordów w zakresie brakujących aktów urodzenia;
- usunięcie, we współpracy z organami gmin, blisko 20 000 sztucznych adresów, tzw. adresów nieznanych;
- codzienna, bieżąca aktualizacja zbioru PESEL na podstawie zgłoszeń użytkowników instytucjonalnych, np. Ministerstwa Finansów, Zakładu Ubezpieczeń Społecznych itp.,
- z odrzutów powstałych na podstawie błędnych aktualizacji przesyłanych z wojewódzkiego zbioru meldunkowego, np. w I kwartale 2015 r. dokonano ręcznie ponad 12 000 aktualizacji danych w zbiorze PESEL, a w całym 2014 r. – ok. 70 000 aktualizacji.

W ramach prowadzonych działań na rzecz poprawy jakości danych po wdrożeniu SRP Minister Cyfryzacji wymieniła:

- weryfikację danych zamieszczonych w raportach rozbieżności, powstałych w wyniku analizy danych przed migracją, których nie można było poprawić systemowo w ramach migracji danych do SRP;
- bieżącą obsługę zgłaszanych rozbieżności w danych, m.in. anulowanie i łączenie podwójnie nadanych numerów PESEL w łańcuch, zmiana numerów PESEL;
- uzupełnienie nieaktualnych kodów TERYT w rejestrze PESEL;
- uzupełnienie brakujących danych w Rejestrze Dowodów Osobistych poprzez ich domigrowanie z Gminnych Ewidencji Wydanych i Unieważnionych Dowodów Osobistych (np. brakujące zdjęcia, daty przyjęcia przez urząd, daty unieważnienia, daty wydania);
- uzupełnienie w Rejestrze Dowodów Osobistych, na podstawie danych z Gminnych Ewidencji Wydanych i Unieważnionych Dowodów Osobistych, brakujących dowodów osobistych, które nie występowały w Ogólnokrajowej Ewidencji Wydanych i Unieważnionych Dowodów Osobistych;
- bieżącą analizę poszczególnych zgłoszeń zamieszczanych przez użytkowników w ITSM *Atmosfera* i podejmowanie odpowiednich działań.

Z *Dokumentacji powykonawczej SRP* opracowanej przez COI wynika, że SRP wykorzystuje przede wszystkim wewnętrzne źródła danych słownikowych[94]. Jedynym słownikiem zewnętrznym, z którego korzysta SRP jest słownik podziału terytorialnego kraju „TERYT" udostępniany przez Główny Urząd Statystyczny. Na podstawie analizy dokumentacji powykonawczej SRP ustalono, że COI opracował aplikację służącą do korzystania z zewnętrznych źródeł danych słownikowych. Aplikacja umożliwia import słowników w określonych formatach z dostępnych źródeł.

Wprowadzenie SRP ujawniło szereg rozbieżności w danych zmigrowanych do SRP. Wdrożone przez COI w SRP mechanizmy weryfikacji danych przyczyniają się do stałej poprawy jakości danych znajdujących się w poszczególnych rejestrach wchodzących w skład SRP.

3.6.2. Weryfikacja prawidłowości danych zgromadzonych w poszczególnych rejestrach wchodzących w skład SRP w urzędach miast/miast i gmin

W okresie od 1 marca 2015 r. do 31 maja 2016 r. w kontrolowanych urzędach stwierdzono, że występowały liczne rozbieżności pomiędzy danymi zgromadzonymi w rejestrach składających się na SRP (PESEL, RDO, BUSC). Rozbieżności te dotyczyły najczęściej:

- w sprawach z zakresu USC:
  - braku nazwiska rodowego wnioskodawcy lub/i ojca wnioskodawcy,
  - błędów w imionach, nazwiskach, miejscu urodzenia i danych rodziców,
  - braku uaktualnienia stanu cywilnego,
  - wskazywania osoby zmarłej jako żyjącej,
- w sprawach z zakresu ewidencji ludności:
  - błędów w kodach pocztowych;
  - błędnych: danych urzędów gmin dokonujących meldunków, nazw ulic, dat wymeldowania, okresów zameldowania;
  - braku danych poprzednich dowodów osobistych;

[94] Zamknięty katalog danych możliwych do wykorzystania w ramach operacji wykonywanych z wykorzystaniem aplikacji „Źródło".

– braku serii, numeru i daty ważności ostatniego wydanego dowodu osobistego;
– niewłaściwego numeru aktu stanu cywilnego lub jego braku.

Analiza próby 683 wniosków[95] składanych przez obywateli w zakresie dowodu osobistego i uzyskania odpisu aktu stanu cywilnego wykazała, że w 122 (18%) przypadkach[96] na etapie weryfikacji wniosków zidentyfikowano rozbieżności zarówno pomiędzy danymi zgromadzonymi w poszczególnych rejestrach wchodzących w skład SRP (PESEL, RDO, BUSC), jak i pomiędzy danymi zawartymi we wnioskach a ww. rejestrami. Ustalenia kontroli wskazują, że we wszystkich przypadkach podejmowano działania mające na celu wyjaśnienie zaistniałych rozbieżności – wysyłano zlecenia usunięcia rozbieżności do właściwych urzędów lub usuwano je we własnym zakresie.

Udostępnione w aplikacji „Źródło" mechanizmy zlecania korekt błędnych danych wpływają na stałą poprawę danych zgromadzonych w rejestrach SRP.

95 UM (w nawiasie: badana próba wniosków): Białystok (45), Bielsk Podlaski (45), Legionowo (37), Krosno (29), Łomża (45), Otwock (45), Piaseczno (45), Przemyśl (44), Rzeszów (45), Świdnica (45), Wałbrzych (45), Warszawa (167) i Wrocław (46).

96 UM (liczba stwierdzonych niezgodności): Białystok (4), Legionowo (2), Piaseczno (12), Przemyśl (1), Rzeszów (10), Świdnica (3), Wałbrzych (5), Warszawa (72), Wrocław (13).

4 INFORMACJE DODATKOWE

4.1 Przygotowanie kontroli

Kontrolę koordynował Departament Administracji Publicznej. Czynności kontrolne zostały przeprowadzone w 14 jednostkach przez cztery jednostki organizacyjne NIK, tj. Departament Administracji Publicznej oraz Delegatury NIK w: Białymstoku, Rzeszowie i we Wrocławiu. Departament Metodyki Kontroli i Rozwoju Zawodowego NIK przeprowadził badanie w zakresie automatycznego unieważniania dowodu osobistego w RDO z wykorzystaniem programu komputerowego ACL służącego do analizy danych.

4.2 Postępowanie kontrolne i działania podjęte po zakończeniu kontroli

Najwyższa Izba Kontroli skierowała 14 wystąpień pokontrolnych do wszystkich kierowników kontrolowanych jednostek. Z danych na dzień 19 stycznia 2017 r. wynika, że na 38 wniosków pokontrolnych sformułowanych przez NIK, 19 zostało zrealizowanych, 18 było w trakcie realizacji, a jeden nie został zrealizowany. Zastrzeżenia do wystąpień pokontrolnych zostały zgłoszone przez dwóch kierowników skontrolowanych jednostek.

Prezydent Miasta Stołecznego Warszawy zgłosiła jedno zastrzeżenie dotyczące stwierdzonej nieprawidłowości polegającej na tym, że komputery, na których wykorzystywana jest aplikacja „Źródło", zarówno w Delegaturze Biura Administracji i Spraw Obywatelskich, jak i w II Wydziale Rejestracji Stanu Cywilnego w Urzędzie Dzielnicy Ochota m.st. Warszawy mają dostęp do sieci Internet. Uchwałą Komisji Rozstrzygającej NIK z dnia 8 listopada 2016 r. oddalono powyższe zastrzeżenie.

Dyrektor COI zgłosiła trzy zastrzeżenia do wystąpienia pokontrolnego. Zastrzeżenia dotyczyły doprecyzowania lub uzupełnienia wystąpienia pokontrolnego o informacje na temat:

– poniesionych przez COI kosztów w wysokości 10 689 tys. zł wynikających z uznania przez COI błędów i braków w funkcjonalnościach SRP,
– wpływu zbyt późnego podłączenia gmin do łącza wydzielonego OST 112 oraz zakończenia dopiero w grudniu 2014 r. zmian przepisów prawnych dotyczących SRP jako przyczyn opóźnień udostępnienia SRP,
– zasad sporządzania miesięcznych raportów z wykonania usług SRP.

Uchwałą Komisji Rozstrzygającej NIK z dnia 19 grudnia 2016 r. oddalono powyższe zastrzeżenia.

W związku z usunięciem nieprawidłowości w trakcie kontroli, NIK odstąpiła od sformułowania wniosku pokontrolnego do Dyrektora Centralnego Ośrodka Informatyki (COI). W wystąpieniu pokontrolnym NIK sformułowała uwagi, które dotyczyły w szczególności:

– zbyt długich okresów rozwiązywania i usuwania incydentów (problemów) związanych z funkcjonowaniem SRP;
– określenia wymaganych parametrów SLA dla wszystkich usług i elementów infrastruktury mających wpływ na dostępność SRP, w tym także serwerowni;
– nie przeprowadzania audytów i testów bezpieczeństwa SRP po jego udostępnieniu, pomimo wprowadzenia licznych zmian w tym systemie.

Dyrektor COI w odpowiedzi na wystąpienie pokontrolne poinformowała m.in., że:

– COI dokłada wszelkich starań aby dostępność systemu SRP była jak najwyższa, a incydenty krytyczne traktowane są priorytetowo, jednak umowne zagwarantowanie wyższej dostępności jest obarczone wysokimi kosztami, co do poniesienia których decyzja jest w gestii Ministerstwa Cyfryzacji;

– COI przekaże do Ministerstwa Cyfryzacji pismo w sprawie potrzeby uregulowania kwestii minimalnego poziomu dostępności serwerowni użyczonych przez MSWiA i Policję;
– przygotowane i testowane jest narzędzie informatyczne do masowej migracji danych o aktach stanu cywilnego, uzgodniono z Ministerstwem Cyfryzacji termin jego wdrożenia produkcyjnego dla pierwszego etapu na 27 stycznia 2017 r., drugi etap przewidziany jest na kwiecień 2017 r.;
– prowadzone są prace nad wdrożeniem systemu zarządzania bezpieczeństwem informacji według normy ISO 27001 oraz ciągłości działania według ISO 22301. Zgodnie z zapowiedziami, prowadzony jest również niezależny audyt bezpieczeństwa systemu SRP.

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

– dokonywania migracji aktów stanu cywilnego do rejestru stanu cywilnego w terminie określonym w art. 125 ust 4 p.a.s.c.;
– wskazywania w zleceniach migracji aktów stanu cywilnego do SRP terminu nieprzekraczającego 10 dni na realizację zlecenia przez inny urząd, stosownie do art. 125 ust. 4 p.a.s.c.;
– uniemożliwienia w sposób trwały dostępu do Internetu na stacjach komputerowych, na których wykorzystywana jest aplikacja „Źródło";
– opracowania i wdrożenia dokumentu polityki bezpieczeństwa informacji określającego zasady bezpieczeństwa informacji, stosownie do § 20 ust. 3 w związku z ust. 1 rozporządzenia KRI;
– wysyłania każdorazowo drogą elektroniczną *potwierdzenia złożenia wniosku o wydanie dowodu osobistego* w przypadku wniosków składanych elektronicznie;
– niezwłocznego odbierania uprawnień użytkownikom aplikacji „Źródło" w chwili zakończenia zatrudnienia lub zmiany zakresu obowiązków;
– przeprowadzania corocznych audytów z zakresu bezpieczeństwa informacji.

NIK zwróciła również uwagę na konieczność popularyzacji wśród obywateli możliwości załatwiania drogą elektroniczną spraw z zakresu wydawania dowodów osobistych i odpisów aktów stanu cywilnego.

Adresaci wystąpień pokontrolnych poinformowali o podjęciu działań na rzecz realizacji wniosków pokontrolnych. Na przykład:

- **Burmistrz Miasta i Gminy Piaseczno** poinformował m.in., że pisemnie zobowiązano naczelnika Wydziału Spraw Obywatelskich do wysyłania każdorazowo *potwierdzenia złożenia wniosku o wydanie dowodu osobistego* w przypadku wniosków składanych elektronicznie, a Kierownika USC do dokonywania migracji aktów stanów cywilnego w terminie określonym w art. 125 ust. 4 p.a.s.c. oraz do wskazywania w zleceniach migracji aktów stanu cywilnego do systemu rejestrów państwowych terminu nieprzekraczającego 10 dni na realizację zlecenia przez inny urząd. Poinformował również, że zobowiązał Kierownika Referatu Informatyki do stałej, bieżącej współpracy z kierownikami jednostek korzystających z SRP w zakresie nadawania uprawnień w aplikacji „Źródło", tak aby uprawnienia były nadawane pracownikom posiadającym stosowne uprawnienia.
- **Prezydent Miasta Otwocka** poinformował m.in., że w Urzędzie będzie przeprowadzany co najmniej raz w roku audyt w zakresie bezpieczeństwa informacji. Podpisana została umowa na przeprowadzenie audytu w 2016 r. – zakończenie umowy 15.12.2016 r. Poinformował również, że na stacjach komputerowych, na których wykorzystywana jest aplikacja „Źródło", uniemożliwiono w sposób trwały dostęp do Internetu.

Charakterystyka stanu prawnego

Prawo o aktach stanu cywilnego

W myśl art. 1 p.a.s.c., ustawa ta reguluje zasady i tryb rejestracji stanu cywilnego oraz dokonywania czynności z zakresu rejestracji stanu cywilnego. Zasadniczym celem ustawy p.a.s.c., która weszła w życie dnia 1 marca 2015 r., było podniesienie jakości rejestracji stanu cywilnego poprzez prowadzenie jej w systemie elektronicznym, co miało pozwolić na:

- odejście od papierowych aktów stanu cywilnego;
- uzyskanie odpisu aktu stanu cywilnego (w tym również w postaci dokumentu elektronicznego) w dowolnym urzędzie stanu cywilnego, niezależnie od miejsca jego przechowywania;
- dostęp kierowników USC do elektronicznych aktów stanu cywilnego, co zwolni osoby zainteresowane z obowiązku przedkładania w urzędach stanu cywilnego odpisów aktów przy dokonywaniu czynności z zakresu rejestracji stanu cywilnego, a kierowników urzędów od przekazywania pocztą informacji o zmianach związanych ze stanem cywilnym;
- zdalną aktualizację przez kierownika USC rejestru PESEL o zdarzeniach z zakresu rejestracji stanu cywilnego, co usprawni aktualizację tego rejestru o dane z zakresu rejestracji stanu cywilnego. W konsekwencji zapewni to prawidłową identyfikację obywatela na podstawie rejestru PESEL.

Zgodnie z art. 2 ust. 2 p.a.s.c. rejestracji stanu cywilnego dokonuje się w rejestrze stanu cywilnego w formie aktów stanu cywilnego. Zatem wszystkie zdarzenia z dziedziny stanu cywilnego są zapisywane i ewidencjonowane wyłącznie w systemie teleinformatycznym, a akty stanu cywilnego sporządzone dotychczas w postaci papierowej są przenoszone stopniowo do systemu elektronicznego. Aktem stanu cywilnego jest wpis o urodzeniu, małżeństwie albo zgonie w rejestrze stanu cywilnego wraz z treścią późniejszych wpisów wpływających na treść lub ważność tego aktu (art. 2 ust. 3 p.a.s.c.). Akt stanu cywilnego jest sporządzony z chwilą dokonania wpisu o urodzeniu, małżeństwie albo zgonie w rejestrze stanu cywilnego (art. 2 ust. 4 p.a.s.c.).

Stosownie do art. 5 ust. 1 i 2 p.a.s.c., rejestr stanu cywilnego jest prowadzony przez ministra właściwego do spraw informatyzacji[97], w systemie teleinformatycznym, a wpisu w rejestrze stanu cywilnego dokonuje kierownik urzędu stanu cywilnego lub zastępca kierownika urzędu stanu cywilnego.

Rejestracja stanu cywilnego jest wykonywana przez gminy w urzędach stanu cywilnego jako zadanie zlecone z zakresu administracji rządowej (art. 6 ust. 1 p.a.s.c.). Zgodnie z art. 6 ust. 3 p.a.s.c. kierownikiem urzędu stanu cywilnego jest wójt (burmistrz, prezydent miasta).

[97] Art. 5 ust. 1 p.a.s.c. został zmieniony z dniem 1 stycznia 2016 r. przez art. 35 pkt 1 lit. a ustawy z dnia 22 grudnia 2015 r. o zmianie ustawy o działach administracji rządowej oraz niektórych innych ustaw (Dz. U. poz. 2281) i stanowi, że rejestr stanu cywilnego jest prowadzony przez ministra właściwego do spraw informatyzacji, w systemie teleinformatycznym. Od dnia 16 listopada 2015 r. ministrem właściwym do spraw informatyzacji jest Minister Cyfryzacji – na podstawie § 1 ust. 2 rozporządzenia Prezesa Rady Ministrów z 17 listopada 2015 r. w sprawie szczegółowego zakresu działania Ministra Cyfryzacji (Dz. U. poz. 1910, ze zm.). Przed 1 stycznia 2016 r. rejestr stanu cywilnego prowadził minister właściwy do spraw wewnętrznych. Zgodnie z § 1 ust. 2 pkt 2 rozporządzenia Prezesa Rady Ministrów z dnia 17 listopada 2015 r. w sprawie szczegółowego zakresu działania Ministra Spraw Wewnętrznych i Administracji, ministrem właściwym do spraw wewnętrznych jest Minister Spraw Wewnętrznych i Administracji (Dz. U. poz. 1897, ze zm.). Wcześniej do dnia 15 listopada 2015 r. ministrem właściwym do spraw wewnętrznych był Minister Spraw Wewnętrznych (§1 ust. 2 rozporządzenia Prezesa Rady Ministrów z dnia 22 września 2014 r., Dz. U. poz. 1265; §1 ust. 2 rozporządzenia Prezesa Rady Ministrów z dnia 18 listopada 2011 r., Dz. U. Nr 248, poz. 1491).

W okręgach liczących powyżej 50 tys. mieszkańców, burmistrz lub prezydent miasta zatrudnia inną osobę na stanowisku kierownika urzędu stanu cywilnego oraz może zatrudnić zastępcę lub zastępców kierownika urzędu stanu cywilnego (art. 6 ust. 5 p.a.s.c.), a w okręgach liczących poniżej 50 tys. mieszkańców zatrudnia zastępcę kierownika USC oraz może zatrudnić inną osobę na stanowisku kierownika urzędu stanu cywilnego (art. 6 ust. 4 p.a.s.c.). Art. 9 ust. 1 p.a.s.c. stanowi, że czynności z zakresu rejestracji stanu cywilnego są dokonywane przez kierownika urzędu stanu cywilnego lub zastępcę kierownika. W myśl art. 10 ust. 1 p.a.s.c. kierownik urzędu stanu cywilnego może upoważnić pisemnie pracownika urzędu stanu cywilnego do wydawania odpisów aktów stanu cywilnego, zaświadczeń o zamieszczonych lub niezamieszczonych w rejestrze stanu cywilnego danych dotyczących wskazanej osoby oraz zamieszczania przypisków (…).

Akty stanu cywilnego stanowią wyłączny dowód zdarzeń w nich stwierdzonych (art. 3 p.a.s.c.). W związku z tym udowodnienie, że akt stanu cywilnego jest niezgodny z prawdą następuje w postępowaniu przed sądem, który dokonuje unieważnienia aktu stanu cywilnego.

Ustawą z dnia 6 lipca 2016 r. o zmianie ustawy–Prawo o aktach stanu cywilnego[98], wprowadzono ponadto dwa różne tryby administracyjnego unieważniania aktów stanu cywilnego. Pierwszy stanowi rozszerzenie dotychczasowych uprawnień wojewody związanych z unieważnianiem aktu stanu cywilnego w drodze decyzji administracyjnej, w sytuacjach gdy doszło do sporządzenia w księgach stanu cywilnego kilku aktów podlegających przeniesieniu do rejestru stanu cywilnego, a stwierdzających to samo zdarzenie. Dotyczy to, zarówno aktów sporządzonych w księgach, przeniesionych do rejestru stanu cywilnego (art. 127 ust. 2 p.a.s.c.), jak też aktów zarejestrowanych już po wejściu w życie ustawy, tj. po dniu 1 marca 2015 r. (art. 39b p.a.s.c.). Drugi tryb pozwala kierownikowi urzędu stanu cywilnego na unieważnianie aktów, które z przyczyn technicznych lub niewłaściwego zastosowania funkcjonalności rejestru stanu cywilnego błędnie zarejestrowano w rejestrze lub też błędnie przeniesiono z papierowej księgi ręcznie albo przy zastosowaniu aplikacji wspierającej. Znajduje on zastosowanie zarówno w ramach rejestracji bieżącej (art. 39a p.a.s.c.[99]) jak i do aktów przenoszonych do rejestru stanu cywilnego, które zostały sporządzone przed dniem 1 marca 2015 r. albo sporządzonych w trybie art. 145 p.a.s.c., w okresie przejściowym do końca sierpnia 2015 r. (art. 127a p.a.s.c.[100]). Uprawnienie kierownika urzędu stanu cywilnego do unieważniania aktów stanu cywilnego przenoszonych z papierowej księgi do rejestru stanu cywilnego rozszerzono o możliwość unieważnienia aktu przeniesionego błędnie na skutek omyłki pisarskiej.

Zgodnie z art. 44 ust. 1 p.a.s.c., kierownik urzędu stanu cywilnego wydaje z rejestru stanu cywilnego:

- odpisy zupełne i odpisy skrócone aktów stanu cywilnego,
- zaświadczenia o zamieszczonych lub niezamieszczonych w rejestrze stanu cywilnego danych dotyczących danej osoby,
- zaświadczenia o stanie cywilnym.

Wniosek o wydanie odpisu aktu stanu cywilnego lub o wydanie zaświadczenia o stanie cywilnym lub zaświadczenia o zmieszczonych lub niezamieszczonych w rejestrze stanu cywilnego danych dotyczących wskazanej osoby składa się do wybranego kierownika urzędu stanu cywilnego (art. 44 ust. 5 p.a.s.c.).

98 Weszła w życie 27 sierpnia 2016 r., z zastrzeżeniem art. 4 tej ustawy.

99 Wszedł w życie 1 października 2016 r.

100 Wszedł w życie 1 października 2016 r.

Zgodnie z art. 124 ust. 1–3 p.a.s.c. akt stanu cywilnego sporządzony w księdze stanu cywilnego prowadzonej na podstawie przepisów obowiązujących przed 1 marca 2015 r., przechowywanej przez kierownika urzędu stanu cywilnego, podlega przeniesieniu do rejestru stanu cywilnego.

Przeniesienie aktu stanu cywilnego do rejestru stanu cywilnego polega na zamieszczeniu w rejestrze stanu cywilnego treści:

1) aktu stanu cywilnego z chwili jego sporządzenia w zakresie wymaganym w niniejszej ustawie;
2) wzmianek dodatkowych, przypisków oraz informacji zawartych w rubryce „uwagi".

Przeniesienie aktu stanu cywilnego do rejestru stanu cywilnego jest czynnością materialno-techniczną.

Od 1 marca 2015 r. każdy akt przenoszony z papierowej księgi stanu cywilnego do rejestru stanu cywilnego wymagał dodatkowego zaangażowania kierownika urzędu stanu cywilnego lub jego zastępcy, który uwierzytelniał ten dokument w systemie.

Ustawą z dnia 6 lipca 2016 r. o zmianie ustawy – Prawo o aktach stanu cywilnego dodany został art. 124a p.a.s.c., który przewiduje możliwość pisemnego upoważnienia pracowników przez kierownika urzędu stanu cywilnego do przenoszenia aktów stanu cywilnego do rejestru stanu cywilnego.

Dane zgromadzone w systemie komputerowym na podstawie przepisów dotychczasowych mogą być wykorzystywane do przenoszenia do rejestru stanu cywilnego aktu stanu cywilnego sporządzonego w księdze stanu cywilnego prowadzonej na podstawie przepisów dotychczasowych (art. 124 ust. 8 p.a.s.c.).

Stosownie do art. 125 p.a.s.c. przeniesienie aktu stanu cywilnego do rejestru dokonywane jest z urzędu w przypadku:

– złożenia wniosku o wydanie odpisu aktu stanu cywilnego,
– złożenia wniosku o wydanie zaświadczenia,
– dokonywania czynności w zakresie rejestracji stanu cywilnego, jeżeli dla jej dokonania niezbędny jest akt stanu cywilnego.

Jeżeli wniosek o wydanie odpisu aktu stanu cywilnego lub o wydanie zaświadczeń został złożony do kierownika urzędu stanu cywilnego, który przechowuje księgę stanu cywilnego prowadzoną na podstawie przepisów dotychczasowych, dokonuje on przeniesienia aktu stanu cywilnego do rejestru stanu cywilnego w terminie umożliwiającym wydanie odpisu lub zaświadczenia w ciągu 7 dni roboczych od dnia złożenia wniosku. (art. 125 ust. 3 p.a.s.c.).

Jeżeli wniosek o wydanie odpisu aktu stanu cywilnego lub o wydanie zaświadczeń został złożony do kierownika urzędu stanu cywilnego, który nie przechowuje księgi stanu cywilnego, przeniesienia aktu stanu cywilnego do rejestru stanu cywilnego dokonuje się w terminie umożliwiającym wydanie odpisu lub zaświadczenia w ciągu 10 dni roboczych od dnia złożenia wniosku (art. 125 ust. 4 p.a.s.c.).

Ustawa z dnia 6 lipca 2016 r. o zmianie ustawy – Prawo o aktach stanu cywilnego wprowadziła istotną zmianę również w tym zakresie. W art. 127b p.a.s.c. przewidziano możliwość wydawania odpisów aktów stanu cywilnego, sporządzonych w księgach stanu cywilnego z wykorzystaniem danych zamieszczonych w aplikacjach wspierających rejestrację stanu cywilnego, prowadzonych przed wdrożeniem rejestru stanu cywilnego, bez konieczności przenoszenia tych aktów do centralnego rejestru. Rozwiązanie to będzie można wykorzystać, w sytuacji gdy:

1) uprawniony podmiot złoży wniosek o wydanie odpisu,

2) nie ma konieczności wprowadzenia zmian w akcie stanu cywilnego, np. zamieszczenia wzmianki dodatkowej o zmianie nazwiska osoby, której akt dotyczy, czy też przypisków przy akcie, a także nie zaistnieje potrzeba uzupełnienia aktu, o którym mowa w art. 124 ust. 4 p.a.s.c., w zakresie niezbędnym do wydania odpisu zgodnego pod względem treści z odpisem, który byłby wydany z rejestru stanu cywilnego.

Właściwym do wydania odpisu z aplikacji wspierających będzie wyłącznie kierownik urzędu stanu cywilnego, przechowujący księgę stanu cywilnego, w której sporządzono akt stanu cywilnego, ponieważ tylko ten organ będzie miał dostęp do aktu, z którego należy wydać odpis. Z rozwiązania tego będzie można skorzystać nie dłużej niż do dnia 1 września 2021 r.

Uprzednio art. 145 p.a.s.c. umożliwiał kierownikowi urzędu stanu cywilnego wykorzystanie dotychczasowych aplikacji do rejestracji stanu cywilnego przez okres 6 miesięcy od dnia wejścia w życie niniejszej ustawy, tj. od dnia 1 marca 2015 r. do dnia 31 sierpnia 2015 r.

Sposób przenoszenia aktów stanu cywilnego sporządzanych w formie papierowej w księgach na podstawie przepisów, które obowiązywały przed dniem 1 marca 2015 r., określa rozporządzenie Ministra Spraw Wewnętrznych z dnia 5 lutego 2015 r. w sprawie przenoszenia aktów stanu cywilnego do rejestru stanu cywilnego[101], wydane na podstawie delegacji ustawowej określonej art. 126 ust. 2 p.a.s.c. Z art. 128 ust. 1 p.a.s.c. wynika, że przeniesieniu podlegają wszystkie akty stanu cywilnego sporządzone w księgach, dla których nie minął okres przechowywania określony nowymi przepisami, tj. odpowiednio 100 lat dla aktów urodzeń oraz 80 lat dla aktów małżeństw i zgonów. Z przepisu tego wynika również, że dla ksiąg stanu cywilnego przechowywanych w urzędzie stanu cywilnego okres, o którym mowa, liczy się od zamknięcia ostatniej księgi, jeżeli zamieszczono w niej wiele roczników.

W rejestrze stanu cywilnego należy zamieścić numer przenoszonego aktu, a po dokonaniu przeniesienia w rejestrze trzeba dokonać uwierzytelnienia tej czynności podpisem elektronicznym. W tym celu należy użyć karty mikroprocesorowej zabezpieczonej kodem PIN (§ 13 i 14 ww. rozporządzenia w sprawie przenoszenia aktów stanu cywilnego do rejestru stanu cywilnego).

Zasady i sposób prowadzenia rejestru stanu cywilnego reguluje rozporządzenie Ministra Spraw Wewnętrznych z dnia 9 lutego 2015 r. w sprawie sposobu prowadzenia rejestru stanu cywilnego oraz akt zbiorowych rejestracji stanu cywilnego[102], wydane na podstawie art. 27 ust. 4 p.a.s.c., które weszło w życie 1 marca 2015 r.

Ustawa o dowodach osobistych

Dowody osobiste wydają organy gmin. Wydawanie, wymiana i unieważnianie dowodów osobistych są zadaniami zleconymi z zakresu administracji rządowej (art. 8 ust. 1 i 2 u.d.o.). Zgodnie z art. 24 ust. 1 i 2 u.d.o. dowód osobisty wydaje się na wniosek, który może zostać złożony w organie dowolnej gminy na terytorium Rzeczypospolitej Polskiej. Wniosek o wydanie dowodu osobistego składa się w formie pisemnej lub w formie dokumentu elektronicznego na zasadach określonych w ustawie o informatyzacji. Wydanie dowodu osobistego następuje nie później niż w terminie 30 dni od dnia złożenia wniosku. W szczególnie uzasadnionych przypadkach termin ten może zostać przedłużony, o czym należy zawiadomić wnioskodawcę (art. 24 ust. 3 i 4 u.d.o.).

[101] Dz. U. poz. 204, ze zm.

[102] Dz. U. z 2016 r. poz. 1904 .

Sposób i tryb składania wniosku o wydanie dowodu osobistego został określony w rozporządzeniu Ministra Spraw Wewnętrznych z dnia 29 stycznia 2015 r. w sprawie wzoru dowodu osobistego oraz sposobu i trybu postępowania w sprawach wydawania dowodów osobistych, ich utraty, uszkodzenia, unieważnienia i zwrotu. Zgodnie z § 10 ust 4 tego rozporządzenia, wnioskodawca otrzymuje potwierdzenie złożenia wniosku o wydanie dowodu osobistego zawierające przewidywaną datę odbioru, odpowiednio w postaci papierowej albo elektronicznej.

Kwestię unieważnienia dowodu osobistego reguluje art. 51 u.d.o. Zgodnie z art. 51 ust. 2 u.d.o. dowód osobisty podlega unieważnieniu z mocy prawa na podstawie przekazanych przez rejestr PESEL do Rejestru Dowodów Osobistych informacji o utracie obywatelstwa polskiego lub zgonie posiadacza dowodu osobistego.

W myśl art. 53 u.d.o. minister właściwy do spraw informatyzacji[103] prowadzi w formie elektronicznej wykaz unieważnionych dowodów osobistych zawierający serie i numery unieważnionych dokumentów oraz serie i numery błędnie spersonalizowanych lub utraconych blankietów dowodów osobistych.

Przepisy zawarte w art. 55 otwierają rozdział 6 u.d.o., zatytułowany „Rejestr Dowodów Osobistych". Rejestr Dowodów Osobistych (RDO) jest publicznym urządzeniem ewidencyjnym służącym do utrwalania danych dotyczących wydanych dowodów osobistych, postępowań w sprawach dowodów osobistych oraz posiadaczy dowodów osobistych. W myśl art. 55 ust. 2 u.d.o. Rejestr Dowodów Osobistych jest rejestrem centralnym prowadzony w formie elektronicznej, co oznacza, że jest tylko jeden taki rejestr. Organem właściwym do prowadzenia RDO jest minister właściwy do spraw informatyzacji[104] (art. 55 ust. 1 u.d.o.). Nie oznacza to jednak, że tylko minister właściwy do spraw informatyzacji jest uprawniony do wprowadzania danych do RDO. Zgodnie z art. 57 ust. 2 u.d.o. organy gmin (wójtowie, burmistrzowie, prezydenci miast) wprowadzają określone dane do RDO. Rejestr Dowodów Osobistych prowadzony jest w postaci elektronicznej. Oznacza to, że nie ma postaci materialnej księgi lub zbioru dokumentów. Jest zbiorem wpisów dokonywanych w formie elektronicznej w sposób pozwalający na ich utrwalenie w postaci wydruku. Dokument wytworzony na podstawie RDO ma walor wtórny – jest wypisem z ewidencji przyjmującym postać uproszczoną.

Art. 57 ust. 1 u.d.o. przewiduje, że organ gminy ma bezpośredni dostęp do danych gromadzonych w RDO. Zgodnie z art. 57 ust. 2 u.d.o., organ gminy (wójt, burmistrz, prezydent miasta) wprowadza do RDO dane bezpośrednio, w czasie rzeczywistym.

Ustawa o ewidencji ludności

Zgodnie art. 2 ustawy z dnia 24 września 2010 r. o ewidencji ludności[105] (dalej u.e.l.) ewidencja ludności polega na rejestracji określonych w ustawie podstawowych danych identyfikujących tożsamość oraz status administracyjnoprawny osób fizycznych. Zgodnie z art. 3 ust. 1 u.e.l.

[103] Przed 1 stycznia 2016 r. właściwy był minister do spraw wewnętrznych. Art. 53 u.o.d. został zmieniony z dniem 1 stycznia 2016 r. przez art. 26 pkt 3 ustawy z dnia 22 grudnia 2015 r. o zmianie ustawy o działach administracji rządowej oraz niektórych innych ustaw (Dz. U. poz. 2281).

[104] Przed 1 stycznia 2016 r. RDO prowadził minister właściwy do spraw wewnętrznych. Art. 55 ust. 1 u.o.d. został zmieniony z dniem 1 stycznia 2016 r. przez art. 26 pkt 5 ustawy z dnia 22 grudnia 2015 r. o zmianie ustawy o działach administracji rządowej oraz niektórych innych ustaw (Dz. U. poz. 2281).

[105] Dz. U. z 2016 r. poz. 722, ze zm.

ewidencję ludności prowadzi się w Powszechnym Elektronicznym Systemie Ewidencji Ludności, który stanowi rejestr PESEL, w rejestrach mieszkańców oraz rejestrach zamieszkania cudzoziemców, prowadzonych w systemie teleinformatycznym.

Stosownie do art. 4 u.e.l. organy gminy wykonują zadania określone w ustawie jako zadania zlecone z zakresu administracji rządowej.

Zgodnie z art. 7 ust. 3 u.e.l. w rejestrze mieszkańców gromadzone są dane osób wskazanych w art. 7 ust. 1 i 2 u.e.l., które wykonały obowiązek meldunkowy na terenie danej gminy.

Zgodnie z art. 10 ust. 4 u.e.l. organy, o których mowa w ust. 1, niezwłocznie dokonują rejestracji danych za pośrednictwem systemu teleinformatycznego. W przypadku braku bezpośredniego dostępu do rejestrów spowodowanego przyczynami niezależnymi od organu rejestracji dokonuje się nie później niż w terminie 2 dni roboczych od dnia, w którym powstał obowiązek ich rejestracji. W przypadku braku możliwości przekazania danych w sposób wskazany w ust. 4 organ przekazuje dane w formie pisemnej w celu ich rejestracji w terminie nie dłuższym niż 4 dni robocze od dnia, w którym powstał obowiązek ich rejestracji (art. 10 ust. 5 u.e.l.).

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

Zgodnie z art. 14 ust. 1 ustawy o informatyzacji podmiot publiczny prowadzący rejestr publiczny jest obowiązany:

1) prowadzić ten rejestr w sposób zapewniający spełnianie minimalnych wymagań dla systemów teleinformatycznych, w przypadku gdy ten rejestr działa przy użyciu systemów teleinformatycznych;
2) prowadzić ten rejestr zgodnie z minimalnymi wymaganiami dla rejestrów publicznych i wymiany informacji w postaci elektronicznej;
3) umożliwić dostarczanie informacji do tego rejestru oraz udostępnianie informacji z tego rejestru drogą elektroniczną, w przypadku gdy ten rejestr działa przy użyciu systemów teleinformatycznych.

Organ administracji rządowej zapewnia działanie rejestru publicznego, używając systemów teleinformatycznych (art. 14 ust. 2 ustawy o informatyzacji).

Podmiot publiczny, organizując przetwarzanie danych w systemie teleinformatycznym, jest obowiązany zapewnić możliwość przekazywania danych również w postaci elektronicznej przez wymianę dokumentów elektronicznych związanych z załatwianiem spraw należących do jego zakresu działania, wykorzystując informatyczne nośniki danych lub środki komunikacji elektronicznej. Podmiot publiczny udostępnia elektroniczną skrzynkę podawczą, spełniającą standardy określone i opublikowane na ePUAP przez ministra właściwego do spraw informatyzacji, oraz zapewnia jej obsługę (art. 16 ust. 1 i 1a ustawy o informatyzacji).

Minimalne wymagania dla rejestrów publicznych i wymiany informacji w postaci elektronicznej zostały określone w rozporządzeniu KRI. Rozporządzenie KRI określa także minimalne wymogi w zakresie bezpieczeństwa informacji.

Bezpieczeństwo informacji

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 warunków umożliwiających realizację i egzekwowanie działań wymienionych § 20 ust. 2 rozporządzenia KRI, w tym 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 (pkt 4);
- bezzwłocznej zmiany uprawnień w przypadku zmiany zadań osób, o których mowa w pkt 4 (pkt 5);
- zapewnienia szkolenia osób zaangażowanych w proces przetwarzania informacji (pkt 6);
- minimalizowania ryzyka utraty informacji w wyniku awarii[106] (pkt 12 lit. b);
- zapewnienia bezpieczeństwa plików systemowych (pkt 12 lit. e);
- zapewnienia okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji, nie rzadziej niż raz na rok (pkt 14).

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 17799 – w odniesieniu do ustanawiania zabezpieczeń[107]; 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.

Centralny Ośrodek informatyki

Centralny Ośrodek Informatyki (COI) został utworzony jako instytucja gospodarki budżetowej na mocy zarządzenia nr 48 Ministra Spraw Wewnętrznych i Administracji z dnia 26 listopada 2010 r. w sprawie utworzenia i nadania statutu instytucji gospodarki budżetowej pod nazwą „Centralny Ośrodek Informatyki"[108].

Zarządzeniem nr 6 Ministra Cyfryzacji z dnia 31 grudnia 2015 r. w sprawie nadania statutu instytucji gospodarki budżetowej pod nazwą „Centralny Ośrodek Informatyki", z dniem 1 stycznia 2016 r. został nadany nowy statut COI. Zgodnie z obowiązującym statutem, funkcję organu założycielskiego i nadzór nad działalnością COI z dniem 1 stycznia 2016 r. sprawuje minister właściwy do spraw informatyzacji (§ 1 ust. 3 oraz § 10 ust. 1). COI posiada osobowość prawną i jest wpisany do rejestru przedsiębiorców Krajowego Rejestru Sądowego (§ 1 ust. 4 i 5).

Przedmiotem podstawowej działalności COI jest m.in. odpłatne wykonywanie na rzecz Ministra usług w zakresie zadań publicznych wynikających z ustaw innych niż ustawa z dnia 20 czerwca 1997 r. – Prawo o ruchu drogowym, regulujących sposób funkcjonowania ewidencji lub rejestrów państwowych innych niż wymienione w pkt 1 statutu COI, a w szczególności wchodzących w skład

[106] Realizacja tego obowiązku następuje poprzez regularne tworzenie i testowanie kopii zapasowych danych i oprogramowania aplikacyjnego, w którym przetwarzane są dane.

[107] Przepis § 20 ust. 3 pkt 1 rozporządzenia KRI został zmieniony z dniem 22 października 2016 r. Dotychczasowa norma PN-ISO/IEC 17799 została zastąpiona normą PN-ISO/IEC 27002.

[108] Dz. Urz. MSWiA Nr 15, poz. 74, ze zm.

Systemu Rejestrów Państwowych: Powszechnego Elektronicznego Systemu Ewidencji Ludności, Rejestru Dowodów Osobistych, Rejestru Stanu Cywilnego oraz innych, a także Centralnej Ewidencji Wydanych i Unieważnionych Dokumentów Paszportowych (§ 2 ust. 2 pkt 2). W myśl § 6 statutu COI uzyskuje przychody:

1) z odpłatnego wykonywania usług na rzecz Ministra;
2) z odpłatnego wykonywania usług na rzecz innych niż Minister podmiotów;
3) ze sprzedaży towarów i składników majątkowych, będących własnością COI;
4) z innych źródeł, w tym z tytułu oprocentowania środków COI zgromadzonych na rachunkach bankowych oraz odsetek i kar umownych naliczanych na podstawie podpisanych umów;
5) z jednorazowej dotacji na pierwsze wyposażenie w środki obrotowe;
6) z dotacji budżetu państwa na realizację zadań publicznych.

Wykaz objętych kontrolą jednostek, osób zajmujących kierownicze stanowiska odpowiedzialnych za kontrolowaną działalność oraz ocen kontrolowanej działalności

Lp.	Nazwa jednostki objętej kontrolą	Osoby odpowiedzialne za kontrolowaną działalność		Ocena kontrolowanej działalności[109]
		Pełniona funkcja	Imię i nazwisko	
Jednostka organizacyjna NIK przeprowadzająca kontrolę – Departament Administracji Publicznej				
1.	Centralny Ośrodek Informatyki	Dyrektor	Monika Jakubiak, od 1 września 2016 r. wcześniej 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 25 stycznia 2016 r.)	O
2.	Urząd Miasta Stołecznego Warszawy	Prezydent Miasta	Hanna Gronkiewicz-Waltz	O
3.	Urząd Miasta Legionowo	Prezydent Miasta	Roman Smogorzewski	O
4.	Urząd Miasta Otwocka	Prezydent Miasta	Zbigniew Szczepaniak	O
5.	Urząd Miasta i Gminy Piaseczno	Burmistrz	Zdzisław Lis	O
Jednostka organizacyjna NIK przeprowadzająca kontrolę – Delegatura NIK w Białymstoku				
6.	Urząd Miejski w Białymstoku	Prezydent Miasta	Tadeusz Truskolaski	O
7.	Urząd Miejski w Łomży	Prezydent Miasta	Mariusz Chrzanowski	O
8.	Urząd Miasta Bielsk Podlaski	Burmistrz	Jarosław Borowski	O
Jednostka organizacyjna NIK przeprowadzająca kontrolę – Delegatura NIK w Rzeszowie				
9.	Urząd Miasta Krosna	Prezydent	Piotr Przytocki	O
10.	Urząd Miejski w Przemyślu	Prezydent	Robert Choma	O
11.	Urząd Miasta Rzeszowa	Prezydent	Tadeusz Ferenc	O
Jednostka organizacyjna NIK przeprowadzająca kontrolę – Delegatura NIK we Wrocławiu				
12.	Urząd Miejski w Świdnicy	Prezydent	Beata Moskal-Słaniewska	O
13.	Urząd Miasta w Wałbrzychu	Prezydent	Roman Szełemej	O
14.	Urząd Miejski Wrocławia	Prezydent	Rafał Dutkiewicz	O

[109] Skrót „O" oznacza „ocena opisowa". NIK zastosowała w wystąpieniach pokontrolnych do kierowników kontrolowanych jednostek opisową formę oceny ogólnej kontrolowanej działalności.

Wykaz najważniejszych aktów prawnych dotyczących kontrolowanej działalności

1. Ustawa z dnia 28 listopada 2014 r. Prawo o aktach stanu cywilnego[110].
2. Ustawa z dnia 6 sierpnia 2010 r. o dowodach osobistych[111].
3. Ustawa z dnia 24 września 2010 r. o ewidencji ludności[112].
4. Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne[113].
5. 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[114].

[110] Dz. U. z 2016 r. poz. 2064 .
[111] Dz. U. z 2016 r. poz. 391, ze zm.
[112] Dz. U. z 2016 r. poz. 722, ze zm.
[113] Dz. U. z 2014 r. poz. 1114, ze zm.
[114] Dz. U. z 2016 r. poz. 113, ze zm.

Wykaz organów, którym przekazano informację o wynikach kontroli

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