NAJWYŻSZA IZBA KONTROLI
Delegatura we Wrocławiu

LWR.410.014.04.2020

Pan
Rafał Gronicz
Burmistrz Zgorzelca

Urząd Miasta Zgorzelec
ul. Bolesława Domańskiego 7
59-900 Zgorzelec

WYSTĄPIENIE POKONTROLNE

P/20/004 – „Realizacja usług publicznych dla obywateli z wykorzystaniem platformy ePUAP”

NAJWYŻSZA IZBA KONTROLI
Delegatura we Wrocławiu
ul. Marszałka J. Piłsudskiego 15/17, 50-044 Wrocław
T +48 71 711 83 00, F +48 71 711 83 50
lwr@nik.gov.pl

I. Dane identyfikacyjne

Jednostka kontrolowana	Urząd Miasta Zgorzelec, ul. Bolesława Domańskiego 7, 59-900 Zgorzelec (dalej: „Urząd")
Kierownik jednostki kontrolowanej	Rafał Gronicz, Burmistrz Zgorzelca, od 4 grudnia 2006 r. (dalej: „Burmistrz")
Zakres przedmiotowy kontroli	Świadczenie przez urzędy j.s.t. e-usług. Rozwiązania organizacyjne i techniczne w zakresie zapewnienia bezpieczeństwa przetwarzania informacji w urzędzie i ich stosowanie.
Okres objęty kontrolą	Od 1 stycznia 2016 r. do zakończenia czynności kontrolnych, tj. 3 sierpnia 2020 r.
Podstawa prawna podjęcia kontroli	Art. 2 ust. 2 ustawy z dnia 23 grudnia 1994 r. *o Najwyższej Izbie Kontroli*[1] (dalej: „ustawa *o NIK"*)
Jednostka przeprowadzająca kontrolę	Najwyższa Izba Kontroli Delegatura we Wrocławiu
Kontroler	Cezary Mazik, główny specjalista kontroli państwowej, upoważnienie do kontroli nr LWR/92/2020 z 23 czerwca 2020 r.

(akta kontroli str. 1-2)

[1] Dz.U. z 2020 r. poz. 1200.

II. Ocena ogólna[2] kontrolowanej działalności

OCENA OGÓLNA

Przyjęte w Urzędzie rozwiązania i zasady świadczenia usług elektronicznych umożliwiły ich sprawną oraz terminową realizację. Niemniej jednak za wyjątkiem ochrony danych osobowych, w Urzędzie nie wprowadzono odpowiednich rozwiązań organizacyjnych w zakresie bezpieczeństwa przetwarzania informacji.

W badanym okresie udostępniono 112 e-usług, w tym 83 za pośrednictwem ogólnopolskiej platformy ePUAP. Rozwój i popularyzacja tego typu usług wynikały z zadań przyjętych w dokumentach strategicznych przez Radę Miejską Zgorzelca i były monitorowane w ramach ich ewaluacji. Informacja o świadczonych usługach drogą elektroniczną była prezentowana w sposób widoczny i czytelny na stronie internetowej Urzędu. Natomiast liczba realizowanych na rzecz obywateli e-usług w I półroczu 2020 r. wyniosła 828, z czego 61% wykonano w ostatnich dwóch miesiącach tego okresu. Przeprowadzone na próbie 20 e-usług badanie wykazało, że były one kierowane do załatwienia bez zbędnej zwłoki, a w przypadku potrzeby uzupełnienia lub korekty przedkładanych dokumentów nie było potrzeby osobistego stawiennictwa w Urzędzie wnioskodawców. We wszystkich wymaganych przepisami sprawach obywatele otrzymywali odpowiedź lub decyzję drogą elektroniczną. W okresie objętym kontrolą Urząd pomocniczo wykorzystywał elektroniczny obieg dokumentów (dalej: „EOD"), zapewniając jednocześnie sprawne i nieprzerwane działanie dedykowanej mu platformy informatycznej. Nie opracowano jednak procedur EOD oraz załatwiania spraw w formie elektronicznej, w tym weryfikacji podpisów elektronicznych przez pracowników.

Urząd posiadał aktualne informacje o zasobach informatycznych jednostki obejmujące ich rodzaj i konfigurację, a uprawnienia użytkowników komputerów objętych oględzinami nie pozwalały na zainstalowanie nieautoryzowanego oprogramowania, co spełniało wymogi określone w przepisach rozporządzenia 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] *(*dalej: *„rozporządzenie KRI").*

W wyniku kontroli NIK stwierdziła nieprawidłowości dotyczące: **[1]** nieopracowania i niewdrożenia systemu zarządzania bezpieczeństwem informacji (dalej: „SZBI"), a w szczególności polityki bezpieczeństwa informacji (dalej: „PBI"), co było niezgodne z § 20 ust. 1 *rozporządzenia KRI;* **[2]** niezapewnienia pełnych szkoleń pracowników w zakresie bezpieczeństwa informacji, co naruszało § 20 ust. 2 pkt 6 *rozporządzenia KRI;* **[3]** udostępnienia osobom nieuprawnionym dokumentu zawierającego techniczne szczegóły stosowanych procedur i zabezpieczeń systemów IT, czym naruszono postanowienia § 20 ust. 2 pkt 7a oraz § 20 ust. 2 pkt. 11 *rozporządzenia KRI;* **[4]** nieprzeprowadzania audytów wewnętrznych w zakresie bezpieczeństwa informacji, co było sprzeczne z § 20 ust. 2 pkt 14 *rozporządzenia KRI;* **[5]** niewyposażenia serwerowni we wszystkie wymagane zabezpieczenia, co naruszało postanowienia § 20 ust. 2 pkt 9 *rozporządzenia KRI.*

[2] Najwyższa Izba Kontroli formułuje ocenę ogólną jako ocenę pozytywną, ocenę negatywną albo ocenę w formie opisowej.
[3] Dz.U. z 2017 r. poz. 2247.

III. Opis ustalonego stanu faktycznego

OBSZAR

1. Świadczenie przez Urząd Miasta Zgorzelec e-usług

Opis stanu faktycznego

1.1. W „Strategii Rozwoju Miasta Zgorzelec na lata 2015-2025”[4] (dalej: „Strategia”), spośród pięciu przyjętych kierunków rozwoju, zawarto kierunek – „Dobre i inteligentne zarządzanie, w tym poprawa jakości i dostępności usług publicznych”. Sformułowano dla niego cel strategiczny: „Miasto zarządzane w sposób inteligentny i zrównoważony” oraz określono cel operacyjny V.I – „Podnoszenie dostępności i jakości usług publicznych”. Jako sposób osiągnięcia tego celu wskazano cztery zadania, w tym zadanie nr 1: „Promowanie i rozwijanie e-usług dla mieszkańców”. W celu realizacji przywołanego zadania przewidziano wprowadzenie rozwiązań informacyjno-technologicznych, które pozwolą mieszkańcom załatwić większość spraw urzędowych bez wychodzenia z domu. Ponadto w Strategii określono mierniki realizacji celu operacyjnego V.I przyjmując, że liczba usług publicznych wykorzystujących technologie IT powinna na koniec 2025 r. wzrosnąć o 100%.

W procesie ewaluacji realizacji Strategii monitorowano wykorzystanie świadczonych e-usług oraz dostępność na rynku nowych rozwiązań technologicznych w zakresie tego rodzaju usług. W wyniku tych działań, przystąpiono do partnerstwa w projekcie „Przyjazny e-urząd – podniesienie jakości usług w zakresie podatków i opłat lokalnych oraz zarządzania nieruchomościami w cześciu Miastach: Stargard, Gryfino, Mińsk Mazowiecki, Głogów, Nowy Targ oraz Zgorzelec”[5] (dalej: „Projekt Przyjazny e-urząd”). Efektem tego było m.in. wdrożenie rozwiązań w zakresie elektronizacji procesu obsługi podatkowej, automatyzacji rozliczeń i poprawy dostępności do informacji o sposobie załatwienia i przebiegu sprawy. Naczelnik Wydziału Funduszy i Rozwoju Urzędu wyjaśnił, że wdrożenie produktów Projektu Przyjazny e-urząd zakończono 31 maja 2020 r., co pozwoliło na uruchomienie lokalnej platformy informatycznej do informowania mieszkańców w obszarze podatków i opłat lokalnych oraz portalu nieruchomości do przekazywania informacji o lokalach użytkowych i nieruchomościach gruntowych przeznaczonych pod inwestycje.

(akta kontroli str. 10-34; 318)

1.2. Według stanu na 15 lipca 2020 r. liczba usług elektronicznych dostępnych dla mieszkańców Gminy Miejskiej Zgorzelec (dalej: „Gmina”) wynosiła 112, z czego w poszczególnych grupach usług świadczono:

- sprawy ogólne – dwie usługi;
- bezpieczeństwo i zarządzanie kryzysowe – dwie usługi;
- budownictwo, architektura, urbanistyka – 11 usług;
- gospodarka komunalna – pięć usług;
- komunikacja, drogownictwo i transport –11 usług;
- kultura, sport, turystyka i oświata – sześć usług;
- nieruchomości, lokale mieszkalne i użytkowe – 18 usług;
- ochrona środowiska – pięć usług;
- podatki i opłaty – 33 usługi;
- sprawy obywatelskie (dowody osobiste, meldunki, wybory) – 13 usług;

[4] Uchwała Nr 143/2016 Rady Miasta Zgorzelec z dnia 29 marca 2016 r. *w sprawie przyjęcia Strategii Rozwoju Miasta Zgorzelec w latach 2015-2025.*

[5] Uchwała Nr 410/2018 Rady Miasta Zgorzelec z dnia 28 sierpnia 2018 r. *w sprawie przystąpienia do partnerstwa w projekcie pn.: „Przyjazny e-urząd – podniesienie jakości usług w zakresie podatków i opłat lokalnych oraz zarządzania nieruchomościami w sześciu Miastach: Stargard, Gryfino, Mińsk Mazowiecki, Głogów, Nowy Targ oraz Zgorzelec”*, planowanym do realizacji w ramach Programu Operacyjnego Wiedza Edukacja Rozwój 2014-2020, Działanie 2.18 Wysokiej jakości usługi administracyjne.

- urodzenia, małżeństwa, zgony – trzy usługi;
- zdrowie i sprawy społeczne – trzy usługi.

Spośród wykazanych wyżej usług elektronicznych 83 udostępniano za pośrednictwem ogólnopolskiej platformy ePUAP, a 29 wytworzonych w ramach projektu Przyjazny e-urząd, za pośrednictwem portalów lokalnych o zasięgu gminnym[6].

Dodatkowo w ewaluacji realizacji Strategii do świadczonych e-usług zaliczano również:

- SMS Zgorzelec – system masowej wysyłki informacji sms do mieszkańców miasta o bieżących sprawach, awariach, wydarzeniach itp.;
- e-dzienniczek – komercyjne rozwiązanie w zakresie elektronicznego dzienniczka ucznia stosowane w szkołach podległych Gminie;
- e-cmentarz – elektroniczna baza danych o cmentarzach na terenie Gminy, oparta o ogólnopolską platformę internetową.

(akta kontroli str. 11-34; 252-275; 318)

1.3. W I półroczu 2020 r. za pośrednictwem ogólnopolskiej platformy ePUAP w Urzędzie na rzecz obywateli zrealizowano 828 usług elektronicznych, z czego:

- 143 usług w okresie od 1 stycznia 2020 r. do 28 lutego 2020 r.;
- 177 usług w okresie od 1 marca 2020 r. do 30 kwietnia 2020 r.;
- 508 usług w okresie od 1 maja 2020 r. do 30 czerwca 2020 r.

Z tych usług 826 (99,8%) świadczonych było w obszarach: sprawy obywatelskie (609 usług); sprawy (pisma) ogólne wpływające do Urzędu (177 usług) oraz urodzenia (40 usług).

Natomiast w badanym okresie mniej niż pięć zrealizowanych usług drogą elektroniczną zanotowano w obszarach: bezpieczeństwo i zarządzanie kryzysowe[7]; budownictwo, architektura, urbanistyka[8]; gospodarka komunalna[9]; komunikacja, drogownictwo i transport[10]; kultura, sport, turystyka, oświata[11]; nieruchomości, lokale mieszkalne i użytkowe[12], podatki i opłaty[13]; ochrona środowiska[14] oraz zdrowie i sprawy społeczne[15].

Zastępca Burmistrza wyjaśnił, że nie prowadzono diagnozy realizacji usług elektronicznych w I półroczu 2020 r., w związku z tym nie były znane przyczyny niskiej realizacji e-usług w tych obszarach.

Wyraźny wzrost liczby świadczonych e-usług w ostatnim z badanych okresów (od 1 maja do 30 czerwieca 2020 r.) nastąpił w związku z odbywającymi się wyborami prezydenckimi. Tego obszaru dotyczyło bowiem 311 zrealizowanych w tym czasie usług elektronicznych[16].

Ponadto istotny wzrost (powyżej 15%) w analizowanych okresach, w stosunku do okresu od 1 stycznia do 28 lutego 2020 r., dotyczył: wniosków o wydanie dowodu

---

[6] Spośród tych usług 28 w obszarze podatków i opłat świadczono za pośrednictwem lokalnego portalu podatkowego zintegrowanego z Węzłem Krajowym (https://podatki.zgorzelec.eu), a jedną usługę z obszaru zarządzania nieruchomości świadczono za pośrednictwem portalu ofert inwestycyjnych (https://mapa.inspire-hub.pl/#/zgorzelec).

[7] Brak zrealizowanych usług elektronicznych w I półroczu 2020 r. na rzecz mieszkańców.

[8] Brak zrealizowanych usług elektronicznych w I półroczu 2020 r. na rzecz mieszkańców.

[9] Brak zrealizowanych usług elektronicznych w I półroczu 2020 r. na rzecz mieszkańców.

[10] Brak zrealizowanych usług elektronicznych w I półroczu 2020 r. na rzecz mieszkańców.

[11] Brak zrealizowanych usług elektronicznych w I półroczu 2020 r. na rzecz mieszkańców.

[12] Zrealizowano łącznie dwie usługi elektroniczne z zakresu nieruchomości w I półroczu 2020 r.

[13] Brak zrealizowanych usług elektronicznych w I półroczu 2020 r. na rzecz mieszkańców.

[14] Brak zrealizowanych usług elektronicznych w I półroczu 2020 r. na rzecz mieszkańców.

[15] Brak zrealizowanych usług elektronicznych w I półroczu 2020 r. na rzecz mieszkańców.

[16] W tym: 18 wniosków o wpisanie do rejestru wyborców; 241 wniosków o wpisanie do spisu wyborców oraz 52 zgłoszenia o zamiarze głosowania korespondencyjnego.

osobistego (wzrost o 50%[17]); zgłoszenia zameldowania lub jego zmiany (wzrost o 69%[18]) oraz zgłoszenia urodzenia dziecka (wzrost o 650%[19]).

(akta kontroli str. 252-275)

1.4. W okresie objętym kontrolą monitoring e-usług realizowanych za pośrednictwem platformy ePUAP prowadzony był wyłącznie w zakresie ewaluacji realizacji Strategii. Dane dla tych potrzeb zbierane były raz w roku i dotyczyły całości usług elektronicznych, bez ich podziału na świadczone na rzecz obywateli oraz przedsiębiorców. Efektem prowadzonego monitoringu realizacji Strategii było podjęcie działań w zakresie pozyskania nowych rozwiązań technologicznych w zakresie e-usług, co zostało opisane w pkt. 1.1. niniejszego wystąpienia pokontrolnego.

(akta kontroli str. 11-31)

1.5. W okresie objętym kontrolą do Urzędu nie wpłynęły skargi i wnioski dotyczące świadczenia usług publicznych w formie elektronicznej lub usprawnienia tej formy komunikacji z kontrolowaną jednostką.

(akta kontroli str. 255)

1.6. Zgodnie z przyjętymi uregulowaniami wewnętrznymi podstawowym sposobem dokumentowania przebiegu załatwiania i rozstrzygania spraw w Urzędzie była forma papierowa[20]. Natomiast w zakresie postępowania kancelaryjnego stosowano instrukcję kancelaryjną ustanowioną przez Prezesa Rady Ministrów dla organów gmin i związków międzygminnych[21] (dalej: „instrukcja kancelaryjna").

Pomocniczo w zakresie dokumentowania przebiegu załatwiania i rozstrzygania spraw funkcjonował także EOD, który wspomagał obsługę platformy ePUAP w oparciu o aplikację IntraDok. Korespondencja przychodząca do jednostki za pomocą ePUAP była widoczna w użytkowanej aplikacji informatycznej. Odbiór elektronicznej korespondencji następował w Punkcie Obsługi Interesanta (dalej: „POI"), gdzie dokonywano także jej rejestracji. Następnie korespondencję przekazywano za pośrednictwem systemu IntraDok do załatwienia do właściwej merytorycznie komórki organizacyjnej Urzędu. W przypadku, gdy korespondencja nie posiadała określonego adresata lub kierowana była do władz Gminy, przekazywana była do Sekretarz Miasta, która dokonywała jej dekretacji. Po otrzymaniu korespondencji kierownik komórki organizacyjnej dokonywał jej wydruku oraz ponownej dekretacji, zakładał w systemie IntraDok sprawę oraz nadawał jej numer z właściwego rejestru. Po wykonaniu tych czynności przekazywał poprzez system IT sprawę do realizacji wyznaczonemu pracownikowi swojej komórki. Pracownik ten badał i rozpoznawał otrzymaną sprawę oraz przygotowywał projekt jej rozstrzygnięcia lub projekt pisma w celu uzupełnienia otrzymanego wniosku. Projekt ten sporządzano w wersji papierowej (tradycyjnej) i przekazywano przełożonemu do akceptacji. Po jego zaakceptowaniu przez przełożonego i złożeniu podpisu na dokumencie, był on skanowany i wysyłany za pośrednictwem systemu IntraDok przez platformę ePUAP. Zeskanowany dokument wysyłany elektronicznie

[17] Z 48 usług w okresie od 1 stycznia do 28 lutego 2020 r. do 72 usług w okresie od 1 maja do 30 czerwca 2020 r.

[18] Z 26 usług w okresie do 1 stycznia do 28 lutego 2020 r. do 44 usług w okresie od 1 marca do 30 kwietnia 2020 r.

[19] Z czterech usług w okresie do 1 stycznia do 28 lutego 2020 r. do 26 usług w okresie od 1 maja do 30 czerwca 2020 r.

[20] Zarządzenie Nr 6/11 Kierownika Urzędu Miasta Zgorzelec z dnia 16 lutego 2011 r. *w sprawie wyboru podstawowego systemu dokumentowania przebiegu załatwiania i rozstrzygania spraw w Urzędzie Miasta Zgorzelec.*

[21] Załącznik nr 1 do rozporządzenia Prezesa Rady Ministrów z dnia 18 stycznia 2011 r. *w sprawie instrukcji kancelaryjnej, jednolitych rzeczowych wykazów akt oraz instrukcji w sprawie organizacji i zakresu działania archiwów zakładowych* (Dz.U. Nr 14, poz. 67).

podpisywano podpisem elektronicznym lub profilem zaufanym wysyłającego. W aktach właściwej komórki organizacyjnej pozostawało oryginalne pismo w formie papierowej. Część pism, np. sygnowane przez Informatyka Urzędu pismo z danymi przekazywanymi do innego podmiotu publicznego, miało postać tylko elektroniczną i było podpisane kwalifikowanym podpisem elektronicznym.

Natomiast w przypadku otrzymania korespondencji drogą tradycyjną (papierowo) dokumenty takie skanowano w POI i kierowano dalej jak korespondencję elektroniczną, przekazując równolegle oryginał korespondencji do właściwej komórki merytorycznej. Pozostałe czynności były takie same jak w przypadku korespondencji otrzymywanej elektronicznie.

NIK zwraca uwagę, że w przypadku dokumentów przesyłanych elektronicznie przez platformę ePUAP, zgodnie z § 59 instrukcji kancelaryjnej, *projekty pism przeznaczone do wysyłki za pomocą środków komunikacji elektronicznej przedstawia się do podpisu wyłącznie w postaci elektronicznej. W przypadku pisma przeznaczonego do wysyłki w postaci elektronicznej podpisujący: podpisuje elektronicznie pismo w postaci elektronicznej; podpisuje odręcznie wydrukowaną treść pisma w postaci elektronicznej (egzemplarz przeznaczony do włączenia do akt sprawy).* Tymczasem jak ustalono w toku kontroli, w Urzędzie pisma przeznaczone do wysyłki drogą elektronicznie podpisane były tradycyjnie, a następnie skanowane i przesyłane za pośrednictwem platformy ePUAP elektronicznie (z podpisem elektronicznym lub profilem zaufanym wysyłającego).

W Urzędzie nie opracowano procedur EOD oraz załatwiania spraw w formie elektronicznej, w tym obejmującej weryfikację podpisów elektronicznych, co opisano w części dotyczącej stwierdzonych nieprawidłowości.

(akta kontroli str. 255-256; 307-309)

Weryfikacja opatrzenia dokumentów elektronicznych wpływających do Urzędu aktualnym podpisem elektronicznym była dokonywana przez pracowników jednostki, z użyciem dostępnych funkcji użytkowanego oprogramowania (Acrobat Reader dla dokumentów PDF w formacie PAdES[22]) lub licencjonowanej aplikacji dedykowanej do weryfikacji podpisów elektronicznych (podpisy XAdES[23]). W przypadku dokumentów wpływających do Urzędu za pośrednictwem Elektronicznej Skrzynki Podawczej z platformy ePUAP, podpisanych profilem zaufanym, uznawano mechanizm weryfikacyjny ePUAP, przyjmując, że w momencie wysyłki dokumentu nie ma możliwości złożenia nieważnego podpisu. Sprawdzeniu podlegało jednak urzędowe potwierdzenie przedłożenia oraz zgodność PESEL wnioskodawcy (weryfikowano, czy dana osoba składa pismo we własnym imieniu).

(akta kontroli str. 309; 334)

Według stanu na 6 lipca 2020 r. pracownicy Urzędu posiadali 12 elektronicznych podpisów kwalifikowanymi oraz 37 profili zaufanych. Dysponowali nimi: Burmistrz i dwóch jego Zastępców, Sekretarz Miasta, Skarbnik Miasta, siedmiu kierowników wydziałów, Kierownik Urzędu Stanu Cywilnego i dwóch jego Zastępców oraz 30 innych pracowników Urzędu[24].

W okresie od 1 stycznia 2020 r. do 30 czerwca 2020 r. narzędziami tymi zostało podpisanych łącznie 1 192 pism.

W toku kontroli nie stwierdzono przypadków złożenia kwalifikowanego podpisu elektronicznego lub zaawansowanego podpisu elektronicznego z wykorzystaniem danych do składania tych podpisów przyporządkowanych do innej osoby.

(akta kontroli str. 248-259; 308-309)

[22] PDF Advanced Electronic Signatures – podpis elektroniczny dokumentów w formacie pdf.
[23] XML Advanced Elektronic Signatures – podpis elektroniczny dokumentów w formacie xml.
[24] W tym: Pełnomocnik ds. informacji niejawnej; główny specjalista, inspektorzy, podinspektorzy oraz referenci.

1.7. Realizacja usług elektronicznych świadczonych przez Urząd w I półroczu 2020 r. na rzecz obywateli została zbadana na próbie 20 e-usług, z których 16 pochodziło z obszaru spraw obywatelskich, a cztery z obszaru spraw (pism) ogólnych kierowanych do Urzędu[25].

Otrzymane za pośrednictwem platformy ePUAP sprawy były kierowane do załatwienia bez zbędnej zwłoki, 16 z nich w dniu wpłynięcia do Urzędu, a cztery w dniu następnym. W 13 przypadkach złożone dokumenty nie wymagały uzupełnienia, a w siedmiu przypadkach Urząd wezwał korzystającego z e-usługi do usunięcia braków lub poprawy formularzy. We wszystkich tych przypadkach wzywano o przedłożenie dokumentów niebędących w posiadaniu Urzędu, np. umów najmu lokali, gdzie wnioskujący chciał się zameldować lub zdjęć spełniających wymagania dla dowodów osobistych. W każdym z tych przypadków wezwanie kierowane było elektronicznie na profil obywatela na ePUAP i nie wymagało osobistego stawiennictwa w siedzibie Urzędu. Tylko w przypadku spraw związanych z wnioskowaniem o wydanie dowodów osobistych system automatycznie komunikował się z Rejestrem Dowodów Osobistych, w pozostałych 13 przypadkach brak było automatycznej komunikacji z innymi systemami IT wykorzystywanymi w Urzędzie. Uzyskanie informacji o stanie aktualnie załatwianej sprawy możliwe było telefonicznie lub e-mailowo, a dodatkowo w przypadku wniosków o wydanie dowodów osobistych obywatele mogli sprawdzić status załatwianej sprawy na portalu obywatel.gov.pl oraz otrzymywali sms z informacją o możliwości odbioru tego dokumentu z Urzędu. W 17 przypadkach, w których realizacja e-usługi wymagała przekazania obywatelowi dokumentu (zaświadczenia, pokwitowania, decyzji), przekazywano go elektronicznie w formie skanu, a proces rozpoznania sprawy przebiegał w sposób opisany w pkt. 1.6. niniejszego wystąpienia pokontrolnego.

(akta kontroli str. 308-309; 337-339)

1.8. Według informacji przekazanych przez Informatyka Urzędu awarie platformy ePUAP w latach 2016-2020 zdarzały się średnio raz na dwa miesiące. Najczęściej dochodziło do nich w okresie wysyłania sprawozdawczości budżetowo-finansowej, pod koniec terminów rozliczania deklaracji PIT oraz w innych okresach wzmożonego wykorzystywania tej platformy. Głównymi objawami awarii było: brak możliwości logowania lub odrzucanie autoryzacji logowania, brak odpowiedzi ze strony serwera oraz brak lub opóźnione sms autoryzacyjne. Urząd nie posiadał informacji, jakie ewentulanie skutki mogły wywołać ww. awarie dla rozpatrywania spraw załatwianych przez obywateli.

(akta kontroli str. 316)

1.9. W okresie objętym kontrolą zapewniono sprawne i nieprzerwane działanie platformy EOD użytkowanej w Urzędzie. W tym celu zawierano corocznie umowy z producentem tego oprogramowania na świadczenie usług serwisu oprogramowania, obejmujące identyfikację i likwidację awarii aplikacji oraz dostosowanie jej do zmian w przepisach prawa opublikowanych w Dziennikach Ustaw[26]. W ramach tych umów producent oprogramowania świadczył usługi wsparcia technicznego w dni robocze w godzinach od 08.00 do 16.00, a awarie aplikacji klasyfikowano jako klasy A[27], klasy B[28] i klasy C[29]. W przypadku

[25] W badanym okresie Urząd nie świadczył usług elektronicznych na rzecz obywateli z obszaru: komunikacja, drogownictwo, transport, geodezja; gospodarka komunalna oraz podatki i opłaty.

[26] Umowa I.271.32.2015 z 4 stycznia 2016 r. obowiązująca do w 2016 r.; Umowa I.271.40.2016 z 28 grudnia 2016 r. obowiązująca w 2017 r.; Umowa I.271.50.2017 z 2 stycznia 2018 r. obowiązująca w 2018 r.; Umowa I.271.51.2018 z 31 grudnia 2018 r. obowiązująca w 2019 r. oraz Umowa I.271.53.2019 z 13 stycznia 2020 r. obowiązująca w 2020 r.

[27] Klasa A – wada uniemożliwiająca działanie systemu spowodowana błędami w aplikacji. Awaria powoduje zaprzestanie funkcjonowania aplikacji.

wystąpienia awarii klasy A czas naprawy wynosił 72 godziny, a w przypadku dostarczenia rozwiązania zastępczego na czas naprawy wzrastał do 14 dni roboczych. Natomiast w przypadku awarii klasy B i C czas naprawy wynosił odpowiednio pięć dni roboczych i 30 dni roboczych, a w przypadku dostarczenia rozwiązania zastępczego na czas naprawy, odpowiednio 28 dni roboczych i „w terminie uzgodnionym z zamawiającym". Zgodnie z zawartymi umowami czas naprawy był liczony od momentu zarejestrowania awarii w systemie Service Desk producenta przez uprawnionego pracownika Urzędu. Za zwłokę wykonawcy w stosunku do wskazanych powyżej terminów przewidziano kary umowne w wysokości 0,1% wynagrodzenia netto za każdy rozpoczęty dzień roboczy opóźnienia oraz możliwość dochodzenia zapłaty odszkodowania uzupełniającego, z zastrzeżeniem, że łączna odpowiedzialność wykonawcy na podstawie umowy nie przekroczy 50% wartości netto wynagrodzenia w niej określonego.

W latach 2016-2020 producent użytkowanej platformy rozwiązywał zgłoszenia, zachowując czasy naprawy zapisane w umowie. W związku z powyższym nie zachodziła przesłanka do obciążania go karami finansowymi.

(akta kontroli str. 164-247; 317)

1.10. Na stronie internetowej Urzędu[30] zamieszczone zostały czytelne informacje o możliwości załatwienia spraw drogą elektroniczną. W jej części centralnej znajdowały się wyraźne przyciski nawigacyjne oznaczone jako „e-urząd" przenoszące na strony poszczególnych usług elektronicznych świadczonych przez Urząd:

- ePUAP – na stronę https://epuap.gov.pl/wps/portal/strefa-klienta, gdzie można było zrealizować usługi elektroniczne dostępne poprzez ogólnokrajową platformę ePUAP;
- obywatel gov.pl – na stronę https://obywatel.gov.pl/, gdzie można realizować usługi elektroniczne dostępne poprzez tą platformę;
- e-dzienniczek – na stronę https://portal.librus.pl/, gdzie można uzyskać dostęp do dzienniczków wszystkich szkół Gminy na platformie komercyjnej;
- e-cmentarz – na stronę https://zgorzelec.grobonet.com/, gdzie można uzyskać informacje i dane na temat cmentarzy zlokalizowanych na terenie Gminy, za pośrednictwem ogólnokrajowej bazy danych;
- miejscowe plany/oferty inwestycyjne – na stronę https://mapa.inspire-hub.pl//#/zgorzelec, gdzie można było zrealizować usługi elektroniczne z zakresu zarządzania nieruchomościami, uruchomione w ramach projektu Przyjazny e-urząd.

Na ww. stronach wykazano listę spraw możliwych do załatwienia w formie e-usług, a w przypadkach w których konieczne było posiadanie profilu zaufanego lub „nowego" dowodu osobistego z warstwą elektroniczną, wskazywano również odpowiednią informację. Ponadto na stronie internetowej Urzędu, oprócz opisanego wyżej przycisku nawigacyjnego „e-usług" dodano także link „Jak załatwić sprawę", który kierował zainteresowanych do zakładki z nazwami grup usług publicznych świadczonych przez Urząd. Po wybraniu którejś z nich korzystający był przenoszony na właściwą podstronę Biuletynu Informacji Publicznej Urzędu[31] (dalej: „BIP") z kartą informacyjną wybranej usługi publicznej.

---

[28] Klasa B – wada, która całkowicie uniemożliwia wykonanie ważnej, pilnej i często występującej operacji w obszarze zastosowań aplikacji. Awaria aplikacji powoduje powstanie wyników o cechach niezgodnych z opisanymi w instrukcji użytkowania i specyfikacji bądź nie funkcjonowania całej aplikacji.

[29] Klasa A – pozostałe wady, które uniemożliwiają lub utrudniają w sposób bezpośredni wykonanie pozostałych funkcji aplikacji oraz wady o niskiej uciążliwości, które nie stanowią zagrożenia wykonania funkcji aplikacji.

[30] www.zgorzelec.eu.

[31] http://bip.um-zgorzelec.dolnyslask.pl/.

Do dnia rozpoczęcia kontroli NIK, na administrowanej przez Urząd stronie internetowej nie zawarto informacji o sposobie uzyskania profilu zaufanego oraz informacji dotyczących „nowego" dowodu osobistego z warstwą elektroniczną. Dopiero w toku kontroli NIK, dodano odpowiedni link „Załóż profil zaufany" obok prezentowanych wyżej e-usług, kierujący korzystającego na stronę: https://www.gov.pl/web/gov/zaloz-profil-zaufany, gdzie można było założyć wskazany profil.

Na stronie internetowej Urzędu brak było odnośnika lub informacji o e-usługach podatkowych wdrożonych w ramach projektu Przyjazny e-urząd. Usługi te były dostępne tylko bezpośrednio na stronie https://podatki.zgorzelec.eu (lokalny portal podatkowy zintegrowany z Węzłem Krajowym[32]). Według informacji udzielonych przez Zastępcę Burmistrza usługa ta będzie promowana w momencie uzupełnienia bazy podatkowej o dane PESEL, co ma nastąpić do 31 grudnia 2020 r.

Podczas wydawania obywatelom dowodów osobistych z warstwą elektroniczną, pracownicy Urzędu informowali mieszkańców o zawartych w dowodzie osobistym certyfikatach, możliwościach jakie one dają oraz o sprawach jakie dzięki nim mogą załatwić. Ponadto obywatele byli instruowani o możliwości zawieszania certyfikatów zawartych w warstwie elektronicznej dowodu osobistego, bez unieważniania blankietu dokumentu.

(akta kontroli str. 304-306; 319; 333)

1.11. W okresie objętym kontrolą przeprowadzono 18 szkoleń z zakresu świadczenia usług drogą elektroniczną, w których wzięło udział 30 pracowników Urzędu.

Ponadto pracownicy Urzędu zapoznawani byli z politykami dotyczącymi ochrony danych osobowych[33] oraz „Instrukcją zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych w Urzędzie Miasta Zgorzelec"[34] (dalej: „Instrukcja zarządzania systemami IT"), co dokumentowano podpisanym oświadczeniem przechowywanym w ich aktach osobowych.

W okresie tym nie zapewniono jednak pełnych szkoleń pracowników w zakresie bezpieczeństwa informacji, co opisano w części dotyczącej stwierdzonych nieprawidłowości.

(akta kontroli str. 256; 278-303; 330-332)

1.12. W Urzędzie nie było opracowanego i wdrożonego SZBI, o którym mowa w § 20 ust. 1 w związku z ust. 3 *rozporządzenia KRI*, co opisano w części dotyczącej stwierdzonych nieprawidłowości.

W okresie objętym kontrolą obowiązywały dokumenty dotyczące bezpieczeństwa danych osobowych. W tym zakresie przyjęto:

- „Politykę bezpieczeństwa systemów informatycznych służących przetwarzaniu danych osobowych w Urzędzie Miasta Zgorzelec"[35], obowiązującą do 7 sierpnia 2017 r.;
- „Politykę bezpieczeństwa przetwarzania danych osobowych w Urzędzie Miasta Zgorzelec"[36], obowiązującą w okresie od 8 sierpnia 2017 r. do 4 grudnia 2018 r.;

[32] Krajowy Węzeł Identyfikacji Elektronicznej, skrótowo nazywany Węzłem Krajowym, to projekt elektronicznego systemu identyfikacji mający służyć obywatelom do szybkiego i zdalnego załatwiania swoich spraw urzędowych.
[33] O których mowa w pkt. 1.12. niniejszego wystąpienia pokontrolnego.
[34] Wprowadzona zarządzeniem Nr 124/104/07 Burmistrza Miasta Zgorzelec z dnia 13 czerwca 2007 r. *w sprawie zatwierdzenia i wdrożenia „Instrukcji zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych w Urzędzie Miasta Zgorzelec* oraz zarządzeniem Nr 610/170/17 Burmistrza Miasta Zgorzelec z dnia 23 listopada 2017 r. w tej samej sprawie.
[35] Wprowadzona zarządzeniem 415/38/05 Burmistrza Miasta Zgorzelec z dnia 7 marca 2005 r. *w sprawie Polityka bezpieczeństwa systemów informatycznych służących przetwarzaniu danych osobowych w Urzędzie Miasta Zgorzelec*.

- „Politykę Ochrony Danych Osobowych w Urzędzie Miasta Zgorzelec”[37], obowiązującą od 5 grudnia 2018 r.;
- „Instrukcję zarządzania systemami IT”.

(akta kontroli str. 35-163)

1.13. W okresie objętym kontrolą w Urzędzie prowadzono jedynie aktualizację dokumentów dotyczących bezpieczeństwa danych osobowych. W związku z nieopracowaniem i niewdrożeniem SZBI oraz nieprowadzeniem audytów wewnętrznych w zakresie bezpieczeństwa informacji, aktualizacja ta nie spełniała wymogów wynikających z § 20 ust. 2 pkt 1 *rozporządzenia KRI*. Przytoczony przepis zobowiązywał bowiem kierownictwo podmiotu publicznego do zapewnienia aktualizacji regulacji wewnętrznych SZBI w zakresie dotyczącym „zmieniającego się otoczenia”.

(akta kontroli str. 35-163)

1.14. Obowiązujące w Urzędzie regulacje w zakresie bezpieczeństwa danych osobowych[38] zawierały także ogólne procedury dotyczące tego obszaru, w zakresie:

- nadawania uprawnień w systemie informatycznym;
- wykorzystywania nośników danych;
- uwierzytelniania i przydziału haseł dla administratorów systemów, użytkowników oraz częstotliwość ich zmiany;
- rozpoczęcia i zakończenia pracy w systemie informatycznym;
- pracy po zaniku napięcia;
- zabezpieczenia systemu informatycznego przed nieautoryzowaną działalnością;
- korzystania z komputerów przenośnych;
- sporządzania i przechowywania kopii zapasowych;
- przygotowywania systemu informatycznego do napraw, przeglądów i konserwacji.

Przytoczone powyżej regulacje zostały w całości opublikowane w formie zarządzenia Burmistrza na stronie BIP, co opisano w części dotyczącej stwierdzonych nieprawidłowości.

(akta kontroli str. 35-163)

1.15. Uprawnieni pracownicy Urzędu posiadali aktualne informacje o zasobach informatycznych jednostki obejmujące ich rodzaj i konfigurację, co spełniało wymogi określone w § 20 ust. 2 pkt 2 *rozporządzenia KRI*.

Wykorzystywane do tego celu oprogramowanie pozwalało na automatyczne wykrywanie sieci, monitorowanie m.in.: serwerów, aplikacji oraz serwisów, inwentaryzowanie oprogramowania i sprzętu, monitorowanie prac użytkowników oraz raportowanie wydajność zasobów sieciowych. Każdy inwentaryzowany w nim element posiadał odrębny rekord i był opisany za pomocą atrybutów.

W toku przeprowadzonych oględzin dokonanych na próbie 15 urządzeń informatycznych[39] stwierdzono, że użytkowany w tym zakresie system wskazywał

---

[36] Wprowadzona zarządzeniem Nr 554/114/17 Burmistrza Miasta Zgorzelec z dnia 8 sierpnia 2017 r. *w sprawie Polityka bezpieczeństwa przetwarzania danych osobowych w Urzędzie Miasta Zgorzelec*.

[37] Wprowadzona zarządzeniem Nr 17/17/18 Burmistrza Miasta Zgorzelec z dnia 5 grudnia 2018 r. *w sprawie zatwierdzenia Polityki Ochrony Danych Osobowych w Urzędzie Miasta Zgorzelec*.

[38] Zarządzenie nr 610/170/17 Burmistrza Miasta Zgorzelec z dnia 23 listopada 2017 r. *w sprawie zatwierdzenia i wdrożenia „Instrukcji zarządzania systemami służącymi do przetwarzania danych osobowych w Urzędzie Miasta Zgorzelec”*.

[39] Tj. 10 komputerów, jednego serwera, jednego routera, dwóch laptopów oraz jednej drukarki.

dla nich aktualne dane[40] dotyczące m.in. zainstalowanego oprogramowania, sprzętu, konfiguracji systemu oraz osoby odpowiedzialnej/użytkownika.

(akta kontroli str. 250-251)

1.16. Uprawnienia użytkowników 10 komputerów objętych oględzinami[41] nie pozwalały na zainstalowanie nieautoryzowanego oprogramowania. Stan ten był zgodny z § 20 ust. 2 pkt 4 *rozporządzenia KRI.*

(akta kontroli str. 250-251)

1.17. Badanie przeprowadzone na próbie 15 pracowników[42], którzy zakończyli zatrudnienie lub zmienili stanowisko pracy (zmienił się ich zakres obowiązków) w latach 2016-2020, wykazało, że wszystkie te osoby miały nieaktywne lub usunięte konta w domenie oraz użytkowanych przez siebie systemach. Likwidacja/dezaktywacja kont była dokonywana przez Informatyków na podstawie przedkładanych kart obiegowych, a kopie tych dokumentów były przez nich przechowywane. W przypadku osoby przeniesionej do pełnienia innych czynności dotychczasowe uprawnienia specyficzne dla poprzedniego stanowiska pracy były zamykane, a na podstawie złożonego wniosku nadane zostały uprawnienia odpowiadające nowemu zakresowi obowiązków. Działanie takie było zgodne z zasadami określonymi w § 20 ust. 2 pkt 5 *rozporządzenia KRI*.

(akta kontroli str. 310-312)

1.18. W badanym okresie w Urzędzie nie przeprowadzano audytów wewnętrznych z zakresu bezpieczeństwa informacji, co opisano poniżej w części dotyczącej stwierdzonych nieprawidłowości.

(akta kontroli str. 252)

Przeprowadzone 28 lipca 2020 r. oględziny serwerowni Urzędu wykazały, że nie spełniały one wszystkich wymogów określonych dla tego typu pomieszczeń, co zostało opisane w sekcji dotyczącej stwierdzonych nieprawidłowości.

(akta kontroli str. 335-336)

Stwierdzone nieprawidłowości

W działalności kontrolowanej jednostki w przedstawionym wyżej zakresie stwierdzono następujące nieprawidłowości:

1. W Urzędzie pomimo powszechnego stosowania EOD jako sposobu pomocniczego w zakresie dokumentowania przebiegu załatwiania i rozstrzygania spraw, nie opracowano procedur EOD oraz załatwiania spraw w formie elektronicznej, w tym weryfikacji podpisów elektronicznych. W ocenie NIK zaniechanie to było działaniem nierzetelnym, gdyż funkcjonujące wewnętrzne uregulowania nie uwzględniały stanu rzeczywistego, tj. pomimo przyjęcia tradycyjnego(papierowego) sposobu dokumentowania, znacząca liczba spraw była dokumentowana elektronicznie w systemie IntraDok.

Zastępca Burmistrza wyjaśnił, że formalnie nie uregulowano procedur w tym zakresie, ale w najbliższym czasie zostanie to wykonane.

(akta kontroli str. 255-256; 307-309; 327-328)

2. W okresie objętym kontrolą w Urzędzie nie zapewniono pełnych szkoleń pracowników w zakresie bezpieczeństwa informacji, uwzględniających m.in.: zagrożenia bezpieczeństwa informacji, skutki naruszenia bezpieczeństwa informacji, w tym odpowiedzialność prawną, co naruszało § 20 ust. 2 pkt 6 *rozporządzenia KRI.*

[40] W przypadku, gdy któreś z urządzeń nie było aktualnie podłączone do sieci, program informował o ostatniej zarejestrowanej konfiguracji oraz informował jak długo urządzenie nie działa lub nie było podłączone do sieci.
[41] W tym: pięciu laptopów oraz pięciu komputerów stacjonarnych.
[42] Z czego 14 osób zakończyło zatrudnienie, a jedna zmieniła stanowisko pracy i zakres wykonywanych obowiązków. Próba ta stanowiła 52% wszystkich osób kończących zatrudnienie lub zmieniających stanowisko pracy (ogółem 29 osób). Sprawdzeniu podlegały konta tych pracowników w domenie, systemie IntraDok oraz systemie finansowo-księgowym SIGID.

Zastępca Burmistrza w wyjaśnieniach wskazał, że pracownicy byli zapoznawani z politykami bezpieczeństwa ochrony danych osobowych oraz „Instrukcją zarządzania systemami IT". NIK wskazuje jednak, że dokumenty te dotyczą przede wszystkim ochrony danych osobowych i obejmują obszar węższy niż bezpieczeństwo informacji, wynikający z przepisów *rozporządzenia KRI*. Zapoznawania ze wskazanymi wyżej dokumentami nie można traktować jako pełnej realizacji szkoleń w tym zakresie.

(akta kontroli str. 256; 278-303; 330-332)

3. W Urzędzie nie opracowano i nie wdrożono SZBI, a w szczególności PBI. Było to niezgodne z wymaganiami § 20 ust. 1 *rozporządzenia KRI*, zgodnie z którymi *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*.

Zastępca Burmistrza wyjaśnił, że w Urzędzie opracowano „Instrukcję zarządzania systemami IT" na podstawie przepisów dotyczących ochrony danych osobowych, opierając się także na wytycznych zawartych w *rozporządzeniu KRI*, nie wskazując jednak tego ostatniego w podstawach prawnych i nie wyodrębniając tej części.

NIK nie podziela stanowiska Zastępcy Burmistrza, ponieważ obszar ochrony danych osobowych jest obszarem węższym niż SZBI, bowiem nie wszystkie przetwarzane informacje zawierają dane osobowe. Ponadto § 20 ust. 3 *rozporządzenia KRI* wskazuje, że wymagania określone w ust. 1 przywołanego rozporządzenia uznaje się za spełnione, jeżeli system zarządzania bezpieczeństwem informacji został opracowany na podstawie Polskiej Normy PN-ISO/IEC 27001 „*Technika informatyczna. Techniki bezpieczeństwa. Systemy zarządzania bezpieczeństwem informacji. Wymagania"* (dalej: „ISO 27001"), a ustanawianie zabezpieczeń, zarządzanie ryzykiem oraz audytowanie odbywa się na podstawie odpowiednich Polskich Norm[43]. Wskazana przez Urząd instrukcja nie spełnia wszystkich wymogów przytoczonych norm.

(akta kontroli str. 35-163; 327)

4. Obowiązująca „Instrukcja zarządzania systemami IT", zawierająca także techniczne szczegóły stosowanych procedur i zabezpieczeń została udostępniona w całości osobom nieuprawnionym, poprzez opublikowanie jej na stronie BIP, jako jednego z zarządzeń Burmistrza. Stwarza to ryzyko, że informacje zawarte w tym dokumencie mogą zostać wykorzystane do przełamania ustanowionych zabezpieczeń. W ocenie NIK działania takie stoją w sprzeczności z postanowieniami § 20 ust. 2 pkt 7a oraz § 20 ust. 2 pkt 11 *rozporządzenia KRI*, które obligują kierownictwo podmiotów publicznych do zapewnienia właściwej ochrony przetwarzanych informacji oraz ustalenia zasad postępowania z informacjami, zapewniających minimalizację wystąpienia ryzyka kradzieży informacji i środków przetwarzania informacji. Ponadto stanowi to naruszenie zasad określonych w załączniku A normy ISO 27001 punkt A.5.1.1, według której szczegóły techniczne zawarte w PBI winne zostać udostępnione wyłącznie odpowiedzialnym pracownikom (nie podlegają one publikacji).

Burmistrz w złożonych wyjaśnieniach poinformował, że publikacja tego aktu wewnętrznego w BIP nastąpiła przez pomyłkę, a 20 lipca 2020 r. został on usunięty

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

i obecnie jest dostępny w całości tylko dla pracowników Urzędu w sieci wewnętrznej intranet.

NIK wskazuje, że dokument w części technicznej wynien być dostępny jedynie dla pracowników realizujących zadania w tym zakresie.

(akta kontroli str. 35-163, 329)

5. W okresie objętym kontrolą w Urzędzie nie przeprowadzano audytów wewnętrznych w zakresie bezpieczeństwa informacji, co było sprzeczne z § 20 ust. 2 pkt 14 *rozporządzenia KRI*, który określał obowiązek wykonywania tego typu audytów co najmniej raz w roku.

Zastępca Burmistrza wyjaśnił, że powodem braku realizacji audytów wewnętrznych w tym zakresie był brak środków finansowych. Poinformował także, że w budżecie Gminy na 2020 r. przewidziano środki na wykonanie audytu zgodności z *rozporządzeniem KRI*.

(akta kontroli str. 252; 320-326)

6. Serwerownie Urzędu, w których gromadzono i przechowywano dane z systemów IT wspomagających świadczenie e-usług, nie były wyposażone w system antywłamaniowy oraz przeciwpożarowy, drzwi przeciwwłamaniowe, a jedna z serwerowni nie miała właściwie zabezpieczonych otworów okiennych, co było niezgodne z pkt 11.1.1 normy PN-ISO/IEC-27002 „*Technika informatyczna – Techniki bezpieczeństwa – Praktyczne zasady zabezpieczania informacji*" i naruszało postanowienia § 20 ust. 2 pkt 9 *rozporządzenia KRI*.

Zastępca Burmistrza w przekazanych wyjaśnieniach wskazał, że spowodowane to było brakiem środków finansowych na ten cel. Poinformował również, że w najbliższym czasie planowane jest zamontowanie kart dostępowych do serwerowni wraz z rejestracją wejść oraz osobnego systemu antywłamaniowego dedykowanego do tych stref, wymiana drzwi na przeciwwłamaniowe oraz wymiana okien na okna antywłamaniowe z szybami P4.

(akta kontroli str. 335-336; 341-342)

IV. Uwagi i wnioski

Uwagi

Najwyższa Izba Kontroli nie formułuje uwag.

W związku ze stwierdzonymi nieprawidłowościami, Najwyższa Izba Kontroli, na podstawie art. 53 ust. 1 pkt 5 ustawy *o NIK*, przedstawia następujące wnioski:

Wnioski

1. Wprowadzenie procedur elektronicznego obiegu dokumentów oraz załatwiania spraw w formie elektronicznej w Urzędzie.

2. Objęcie pracowników Urzędu stosownymi szkoleniami w zakresie bezpieczeństwa informacji.

3. Opracowanie i wdrożenie systemu zarządzania bezpieczeństwem informacji, zgodnie z § 20 ust. 1, w związku z ust. 3 *rozporządzenia KRI*.

4. Ograniczenie upowszechniania polityki bezpieczeństwa informacji wyłącznie do części deklaratywnej tego dokumentu.

5. Zapewnienie dostępu do części technicznej polityki bezpieczeństwa informacji wyłącznie pracownikom odpowiedzialnym za jej realizację.

6. Zapewnienie przeprowadzania audytów wewnętrznych z zakresu bezpieczeństwa informacji, zgodnie z wymogami § 20 ust. 2 pkt 14 *rozporządzenia KRI*.

7. Zabezpieczenie serwerowni Urzędu w sposób odpowiadający wymogom *rozporządzenia KRI,* w tym normy PN-EN ISO/IEC 27002.

V. Pozostałe informacje i pouczenia

Wystąpienie pokontrolne zostało sporządzone w dwóch egzemplarzach; jeden dla kierownika jednostki kontrolowanej, drugi do akt kontroli.

Prawo zgłoszenia zastrzeżeń

Zgodnie z art. 54 ustawy *o NIK* kierownikowi jednostki kontrolowanej przysługuje prawo zgłoszenia na piśmie umotywowanych zastrzeżeń do wystąpienia pokontrolnego, w terminie 21 dni od dnia jego przekazania. Zastrzeżenia zgłasza się do dyrektora Delegatury NIK we Wrocławiu. Prawo zgłaszania zastrzeżeń, zgodnie z art. 61b ust. 2 ustawy *o NIK*, nie przysługuje do wystąpienia pokontrolnego zmienionego zgodnie z treścią uchwały w sprawie zastrzeżeń.

Obowiązek poinformowania NIK o sposobie wykonania wniosków

Zgodnie z art. 62 ustawy *o NIK* należy poinformować Najwyższą Izbę Kontroli, w terminie 21 od otrzymania wystąpienia pokontrolnego, o sposobie wykonania wniosków pokontrolnych oraz o podjętych działaniach lub przyczynach niepodjęcia tych działań.

W przypadku wniesienia zastrzeżeń do wystąpienia pokontrolnego, termin przedstawienia informacji liczy się od dnia otrzymania uchwały o oddaleniu zastrzeżeń w całości lub zmienionego wystąpienia pokontrolnego.

Wrocław, października 2020 r.

Najwyższa Izba Kontroli
Delegatura we Wrocławiu
p.o. Dyrektor
Marcin Kaliński

.....
podpis

Kontroler
Cezary Mazik
Główny specjalista kontroli państwowej

.....
podpis