WOJEWODA OPOLSKI

Opole, 8 października 2025 r.
PN.I.431.4.3.2025.NL

Pan
Sebastian Baca
Wójt Gminy Branice
Urząd Gminy w Branicach
ul. Słowackiego 3
48-140 Branice

WYSTĄPIENIE POKONTROLNE

I. Dane identyfikacyjne kontroli

1. Nazwa i adres jednostki kontrolowanej: Urząd Gminy w Branicach, ul. Słowackiego 3, 48-140 Branice[1];
2. Podstawa prawna podjęcia kontroli:
   a) Art. 25 ust. 1 pkt 3 lit. a i ust. 3 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (t.j. Dz.U. z 2024 r. poz. 1557 ze zm.)[2],
   b) Art. 6 ust. 4 pkt 3 ustawy z dnia 15 lipca 2011 r. o kontroli w administracji rządowej (t.j. Dz.U z 2020 r. poz. 224 ze zm.)[3];
3. Zakres kontroli:
   a) Przedmiot kontroli: Działanie systemów teleinformatycznych i rejestrów publicznych używanych do realizacji zadań zleconych z zakresu administracji rządowej,

[1] UG w Branicach
[2] Dalej: ustawa o informatyzacji działalności podmiotów
[3] Dalej: ustawa o kontroli

b) Okres objęty kontrolą: od 1 stycznia 2025 r. do dnia rozpoczęcia kontroli (z uwzględnieniem okresu wcześniejszego i późniejszego w zakresie niezbędnym do realizacji celu kontroli);

4. Rodzaj kontroli: problemowa;
5. Tryb kontroli: zwykły;
6. Termin kontroli: 21 lipca 2025 r. – 4 sierpnia 2025 r., kontrola prowadzona była w trybie hybrydowym, tj. dnia 21 lipca 2025 r. – rozpoczęcie czynności kontrolnych w UG w Branicach oraz oględziny serwerowni na miejscu w jednostce. Pozostałe dni (22 lipca – 4 sierpnia 2025 r.) kontrola prowadzona była zdalnie;
7. Skład zespołu kontrolnego:
   a) Natalia Lenart – Inspektor Wojewódzki w Oddziale Organizacji, Kontroli i Skarg w Wydziale Prawnym i Nadzoru w Opolskim Urzędzie Wojewódzkim – kierownik zespołu kontrolnego,
   b) Agnieszka Orlińska-Gocka - Inspektor Wojewódzki w Oddziale Organizacji, Kontroli i Skarg w Wydziale Prawnym i Nadzoru w Opolskim Urzędzie Wojewódzkim – członek zespołu kontrolnego,
   c) Kamil Dziechciński - Starszy Specjalista w Oddziale Informatyki i Rozwoju w Biurze Obsługi Urzędu w Opolskim Urzędzie Wojewódzkim – członek zespołu kontrolnego;
8. Kierownik jednostki kontrolowanej: Pan Sebastian Baca – Wójt Gminy Branice, od dnia 6 maja 2024 r.[4]
9. Kontrolę wpisano do książki kontroli prowadzonej w jednostce kontrolowanej, pod poz. nr 4/2025.

II. Ocena skontrolowanej działalności, ze wskazaniem ustaleń, na których została oparta

Działanie systemów teleinformatycznych i rejestrów publicznych używanych do realizacji zadań zleconych z zakresu administracji rządowej, w okresie od 1 stycznia 2025 r. do dnia rozpoczęcia kontroli (z uwzględnieniem okresu wcześniejszego i późniejszego w zakresie niezbędnym do realizacji celu kontroli), tj. 21 lipca 2025 r. w Urzędzie Gminy w Branicach ocenia się negatywnie.

[4] Akta kontroli - Podpisana dokumentacja kontrolna: Zaświadczenie o wyborze, Ślubowanie, str. 50-321

W trakcie kontroli zostały stwierdzone nieprawidłowości i uchybienia w dużej ilości, które mają zdecydowany wpływ na zapewnienie bezpieczeństwa informacji[5], co uniemożliwia postawienie oceny pozytywnej.

W kontrolowanym okresie zakres działania i zadania oraz organizację i zasady funkcjonowania UG w Branicach określał Regulamin organizacyjny Urzędu Gminy w Branicach[6] stanowiący załącznik do Zarządzenia nr 38U/24 Wójta Gminy Branice z dnia 16 maja 2024 r. w sprawie ustalenia Regulaminu Organizacyjnego Urzędu Gminy w Branicach[7].

Zgodnie z § 5 pkt 2 rozdziału III Regulaminu organizacyjnego – struktura organizacyjna Urzędu Gminy - Kierownikiem Urzędu w rozumieniu przepisów o samorządzie gminnym jest Wójt.

Osobą pełniącą funkcję Administratora Systemów Informatycznych[8] jest Pracownik na stanowisku ds. informatyki i obsługi urzędowych stron internetowych.[9]

Osobą odpowiedzialną za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa jest Pracownik na samodzielnym stanowisku ds. informatyki i obsługi urzędowych stron internetowych. Zgłoszenie osoby do CSIRT NASK nastąpiło dnia 4 marca 2021 roku.[10] Podkreślić należy fakt, że nakładająca powyższy obowiązek ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa[11], weszła w życie w dniu 28 sierpnia 2018 r.

Zgodnie z Komentarzem do ustawy o krajowym systemie cyberbezpieczeństwa: „Prawodawca użył w komentowanym artykule zwrotu „wyznacza osobę”. Zgodnie ze słownikowym znaczeniem, podmiot publiczny ma wskazać osobę do określonego zadania. Prawodawca nie określił formy, w jakiej należy wyznaczyć tę osobę. Podmiot publiczny musi zatem wykazać, iż dokonał czynności wyznaczenia osoby do tego zadania, a osoba ta przyjęła tę funkcję. Formą wyznaczenia może być zarówno umowa o pracę, aneks do umowy powierzający pełnienie tej funkcji lub też zawarcie odrębnej umowy, gdy usługi takie mają być realizowane na innej podstawie

[5] Dalej: BI
[6] Dalej: Regulamin organizacyjny, aktualizowany zarządzeniem nr 47U/25 Wójta Gminy Branice z dnia 26 czerwca 2025 r. zmieniające zarządzenie w sprawie ustalenia Regulaminu Organizacyjnego Urzędu Gminy w Branicach (Akta kontroli - Podpisana dokumentacja kontrolna: Zmiana Regulaminu Organizacyjnego, str. 50-321)
[7] Akta kontroli - Podpisana dokumentacja kontrolna: Regulamin Organizacyjny, str. 50-321
[8] Dalej: ASI
[9] Akta kontroli - Podpisana dokumentacja kontrolna: Zakres obowiązków J.K., Zarządzenie ASI, str. 50-321
[10] Akta kontroli - Podpisana dokumentacja kontrolna: zgłoszenie do CSIRT NASK, str. 50-321
[11] (t.j. Dz.U. z 2024 r. poz. 1077 ze zm.), dalej: ustawa o krajowym systemie cyberbezpieczeństwa

świadczenia pracy."[12] W związku z brakiem umocowania pisemnego przekazania funkcji osoby kontaktowej, zespół kontrolny zwrócił się o złożenie wyjaśnień. Wynika z nich, że pracownik na stanowisku ds. informatyki i obsługi urzędowych stron internetowych do wykonywania funkcji osoby kontaktowej został upoważniony w formie ustnej. Brak umocowania wskazanego zadania poprzez wyznaczenie oraz przyjęcie funkcji przez odpowiedzialnego pracownika, zostaje stwierdzone jako uchybienie. Niemniej jednak, w trakcie trwania kontroli, zostało sporządzone zarządzenie nr 55U/25 Wójta Gminy Branice z dnia 24 lipca 2025 r. w sprawie wyznaczenia osoby odpowiedzialnej za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa w Urzędzie Gminy w Branicach, które reguluje powyższe kwestie przekazania funkcji osoby kontaktowej pracownikowi[13]. W związku z powyższym, przedmiotowa sprawa nie zostanie poddana ocenie.

W UG w Branicach do realizacji zadań zleconych z zakresu administracji rządowej wykorzystywanych jest 5 systemów teleinformatycznych[14], w tym:

- 2 o zasięgu krajowym;
- 3 o zasięgu lokalnym.

1. Elektroniczna skrzynka podawcza

Podstawa prawna:

- Art. 16 ust. 1a ustawy o informatyzacji działalności podmiotów: Podmiot publiczny udostępnia elektroniczną skrzynkę podawczą, spełniającą standardy określone i opublikowane na ePUAP przez ministra właściwego do spraw informatyzacji, oraz zapewnia jej obsługę.

Na stronie głównej Biuletynu Informacji Publicznej[15] UG w Branicach została udostępniona Elektroniczna Skrzynka Podawcza[16]: /ugb3/SkrytkaESP, znajdująca się na Elektronicznej Platformie Usług Administracji Publicznej[17], pozwalająca na wysyłanie i odbieranie pism w formie dokumentów elektronicznych. Dodatkowo w BIP został udostępniony adres do doręczeń elektronicznych, tj. AE:PL-81278-20984-IAUFE-11, który UG w Branicach posiada zgodnie z art. 8 ustawy z dnia

[12] K. Czaplicki (red.), A. Gryszczyńska (red.), G. Szpor (red.), Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz
[13] Akta kontroli - Pismo z wyjaśnieniami dot. pkt 5, str. 47, Akta kontroli - Wyjaśnienia dot. kontroli wraz z podpisaną dokumentacją: Zarządzenie w sprawie wyznaczenia osoby odpowiedzialnej za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa, str. 326-330
[14] Akta kontroli - Zestawienie systemów teleinformatycznych, str. 11-13
[15] Dalej: BIP
[16] Dalej: ESP
[17] Akta kontroli - Podpisana dokumentacja kontrolna: Wniosek o aktywowanie platformy ePUAP, str. 50-321, Dalej: ePUAP

18 listopada 2020 r. o doręczeniach elektronicznych (t.j. Dz.U. z 2024 r. poz. 1045 ze zm.).

2. Obieg dokumentów elektronicznych w urzędzie

Podstawa prawna:

- § 19 ust. 2 pkt 9 Rozporządzenia Rady Ministrów z dnia 21 maja 2024 r. w sprawie krajowych ram interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych[18]: Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez: zabezpieczenie informacji w sposób uniemożliwiający nieuprawnionemu jej ujawnienie, modyfikacje, usunięcie lub zniszczenie.

Wykorzystanie systemu elektronicznego w zakresie zarządzania dokumentami elektronicznymi poprawia przepływ dokumentów w Urzędzie oraz usprawnia przeprowadzenie archiwizacji, co wpływa na przyspieszenie załatwianych spraw oraz wzrost poziomu BI. Zastosowanie systemu teleinformatycznego wspomagającego elektroniczny obieg dokumentów pozwala na realizację interfejsów z innymi systemami podmiotu publicznego w celu przekazywania dokumentów pomiędzy tymi systemami w postaci elektronicznej.

W UG w Branicach podstawowym sposobem dokumentowania przebiegu załatwiania i rozstrzygania spraw jest tradycyjny (tj. papierowy) system wykonywania czynności kancelaryjnych[19].

3. Dokumenty z zakresu bezpieczeństwa informacji; zaangażowanie kierownictwa podmiotu.

Podstawa prawna:

- § 19 ust. 1 rozporządzenie KRI: 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;
- § 19 ust. 2 rozporządzenie KRI: Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienie przez kierownictwo

[18] Dz.U. z 2024 r. poz. 773, dalej: Rozporządzenie KRI
[19] Akta kontroli - Protokół oględzin serwerowni, str. 332-335

podmiotu publicznego warunków umożliwiających realizację i egzekwowanie działań związanych z bezpieczeństwem informacji;

- § 19 ust. 2 pkt 1 rozporządzenie KRI: Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez: zapewnienie aktualizacji regulacji wewnętrznych w zakresie dotyczącym zmieniającego się otoczenia.

Zgodnie z zapisami rozporządzenia KRI, podmiot publiczny realizujący zadania publiczne powinien opracować dokumentację Systemu Zarządzania Bezpieczeństwem Informacji[20], w tym regulacje wewnętrzne oraz zapewnienie ich aktualizacji zgodnie ze zmieniającym się otoczeniem. Kompleksowa dokumentacja SZBI jest warunkiem niezbędnym do skutecznego zarządzania bezpieczeństwem informacji w Urzędzie.

Podstawowym elementem SZBI jest Polityka Bezpieczeństwa Informacji[21], która zgodnie z § 2 pkt 15 rozporządzenia KRI stanowi zestaw efektywnych, udokumentowanych zasad i procedur bezpieczeństwa wraz z ich planem wdrożenia i egzekwowania. PBI zazwyczaj zawiera wyrażoną przez kierownictwo deklarację stosowania, opisuje organizację i ustala osoby odpowiedzialne oraz ich zakresy odpowiedzialności, wprowadza klasyfikacje informacji, sposób postępowania z poszczególnymi rodzajami informacji. Dodatkowo może określać aktywa oraz ich właścicieli, oraz sposób szacowania ryzyka i postępowania z ryzykiem.

System SZBI winien być na bieżąco monitorowany i poddawany przeglądom, celem udoskonalenia go. Czynności te powinny znaleźć odzwierciedlenie w dokumentacji systemu.

W UG w Branicach nie został opracowany i ustanowiony, wdrożony i eksploatowany, monitorowany i przeglądany oraz utrzymywany i doskonalony SZBI.

Obecnie w UG w Branicach stosowana jest Polityka bezpieczeństwa danych osobowych Urzędu Gminy w Branicach[22] wprowadzona Zarządzeniem nr 33 U Wójta Gminy Branice z dnia 25 maja 2018 r. w sprawie wprowadzenia „Polityki bezpieczeństwa danych osobowych Urzędu Gminy w Branicach[23]. Jednakże

[20] Dalej: SZBI
[21] Dalej: PBI
[22] Dalej: PBDO
[23] Akta kontroli - Podpisana dokumentacja kontrolna: Polityka bezpieczeństwa danych osobowych wraz z załącznikami, Załącznik nr 4 do polityki bezpieczeństwa aktualizacja, str. 50-321, dalej: zarządzenie w sprawie wprowadzenia „Polityki bezpieczeństwa danych osobowych Urzędu Gminy w Branicach”

z dokumentacji kontrolnej nie wynika, aby zarządzenie to było monitorowane, poddawane przeglądom ani doskonalone.

W UG w Branicach pracownicy po zapoznaniu się z „Instrukcją zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Gminy w Branicach”[24] oraz procedurami obowiązującymi w Urzędzie, podpisują oświadczenia o przestrzeganiu wymagań dotyczących bezpieczeństwa informacji oraz o zaznajomieniu się z przepisami dot. ochrony danych osobowych[25].

W zakresie dokumentacji z zakresu BI, zespół kontrolny stwierdził dwie nieprawidłowości. Pierwszą z nich jest brak opracowania, ustanowienia, wdrożenia i eksploatowania, monitorowania i przeglądania oraz utrzymania i doskonalenia SZBI. Natomiast druga to brak przeprowadzania przeglądów zarządzenia w sprawie wprowadzenia „Polityki bezpieczeństwa danych osobowych Urzędu Gminy w Branicach”.

4. Analiza zagrożeń związanych z przetwarzaniem informacji

Podstawa prawna:

- § 19 ust. 2 pkt 3 rozporządzenie KRI: Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez: przeprowadzanie okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji oraz podejmowanie działań minimalizujących to ryzyko, stosownie do wyników przeprowadzonej analizy.

Wymogiem skuteczności SZBI jest przeprowadzanie okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji. Kluczowa rola analizy ryzyka wynika z faktu, że rodzaj i poziom zastosowanych zabezpieczeń jest względny oraz zależny od ważności aktywów informatycznych danego podmiotu. Proces szacowania ryzyka powinien być przeprowadzony i udokumentowany w celu wykazania, że ryzyko zostało zidentyfikowane, oszacowane i wprowadzono odpowiednie środki obrony. Szacowanie ryzyka pozwala na aktywne zarządzanie BI, w tym przeciwdziałanie zagrożeniom, ograniczenie skutków zmaterializowanych ryzyk oraz racjonalne zarządzenie środkami finansowymi poprzez stosowanie zabezpieczeń adekwatnych do istniejącego poziomu ryzyka.

[24] Dalej: IZSI

[25] Akta kontroli - Podpisana dokumentacja kontrolna: Oświadczenia pracowników o przestrzeganiu wymagań dot. BI, Oświadczenia pracowników o zaznajomieniu się z przepisami dot. ochrony danych osobowych, str. 50-321

Jednocześnie należy zaznaczyć, że prawidłowość przeprowadzenia analizy ryzyka polega na jego regularnym i ciągłym monitorowaniu.

Analiza ryzyka bezpieczeństwa informacji, mająca na celu identyfikację zagrożeń, oszacowanie ryzyka i określenie środków zaradczych dla zapewnienia poufności, integralności i dostępności informacji przetwarzanych w UG w Branicach, została przeprowadzona w 2024 r. przez IOD.[26]

5. Inwentaryzacja sprzętu i oprogramowania informatycznego

Podstawa prawna:

- § 19 ust. 2 pkt 2 rozporządzenie KRI: Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez: utrzymywanie aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji obejmującej ich rodzaj i konfigurację.

Zarządzenie infrastrukturą informatyczną wymaga utrzymywania aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji obejmującej ich rodzaj i konfigurację. W przedmiotowym spisie winny być wykazane wszystkie zidentyfikowane aktywa informatyczne wraz z najistotniejszymi informacjami o nich. Stworzona baza ma na celu podejmowanie właściwych decyzji i działań w zakresie zmian w środowisku teleinformatycznym.

W dokumentacji przekazanej przez UG w Branicach znajdują się zestawienia sprzętu komputerowego oraz informatycznego, zawierające nazwę, numer seryjny i osobę użytkującą. Dodatkowo sporządzone zostało zestawienie oprogramowań informatycznych, określające ich nazwę, opis funkcji oraz producenta. Przedmiotowe dokumenty wskazują na utrzymanie aktualności posiadanego sprzętu oraz oprogramowania [27].

6. Zarządzanie uprawnieniami do pracy w systemach informatycznych

Podstawa prawna:

- § 19 ust. 2 pkt 4 rozporządzenie KRI: Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności 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 mających na celu zapewnienie bezpieczeństwa informacji;

[26] Akta kontroli - Podpisana dokumentacja kontrolna: Analiza Ryzyka, str. 50-321
[27] Akta kontroli - Podpisana dokumentacja kontrolna: Inwentaryzacja sprzętu, Oprogramowanie informatyczne, Zestawienie sprzętu komputerowego, str. 50-321

- § 19 ust. 2 pkt 5 rozporządzenie KRI: Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez: bezzwłoczną zmianę uprawnień, w przypadku zmiany zadań osób, o których mowa w pkt 4.

Kluczowym elementem polityki BI jest zarządzanie dostępem do systemów teleinformatycznych przetwarzających informacje. Zarządzenie dostępem ma zapewnić, 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 lub zakończenia stosunku pracy następuje zmiana lub odebranie uprawnień.

Pracownicy UG w Branicach realizujący zadania zlecone z zakresu administracji rządowej posiadają upoważnienia do przetwarzania informacji wraz z odpowiednimi uprawnieniami w systemach, które zgodne są z ich zakresami czynności[28].

Wójt Gminy Branice wyjaśnił, że w okresie objętym kontrolą nie było przypadków nadania/zmiany/cofania uprawnień dostępu do systemów[29].

Dodatkowo z informacji uzyskanej od Wójta Gminy Branice wynika, że wnioski o nadanie/zmianę/cofnięcie uprawnień dostępu do systemów, składane są w formie ustnej[30]. Działanie to narusza wytyczne określone w § 5 pkt 12 PBDO. W związku z powyższym, zespół kontrolny stwierdza uchybienie.

7. Szkolenia pracowników zaangażowanych w proces przetwarzania informacji

Podstawa prawna:

- § 19 ust. 2 pkt 6 rozporządzenie KRI: Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez: zapewnienie szkolenia osób zaangażowanych w proces przetwarzania informacji ze szczególnym uwzględnieniem takich zagadnień, jak: a) zagrożenia bezpieczeństwa informacji, b) skutki naruszenia zasad bezpieczeństwa informacji, w tym odpowiedzialność prawna, c) stosowanie środków zapewniających bezpieczeństwo informacji, w tym urządzenia i oprogramowanie minimalizujące ryzyko błędów ludzkich.

[28] Akta kontroli - Podpisana dokumentacja kontrolna: Uprawnienia do programów podatkowych, Upoważnienia do przetwarzania danych osobowych, uprawnienia CEIDG, zakresy czynności, str. 50-321
[29] Akta kontroli - Wyjaśnienia dot. kontroli wraz z podpisaną dokumentacją: wyjaśnienia dot. pkt 1, str. 326-330
[30] Akta kontroli - Pismo z wyjaśnieniami dot. pkt 6, str. 48

Szkolenia podnoszące świadomość zagrożeń i konsekwencji zaistnienia incydentów związanych z BI winny obejmować wszystkie osoby uczestniczące w procesie przetwarzania informacji. Z uwagi na stale zmieniające się zagrożenia BI oraz zabezpieczenia przed takimi incydentami, szkolenia osób zaangażowanych w proces przetwarzania informacji powinny być przeprowadzane cyklicznie.

W 2024 r. w UG w Branicach dla osób zaangażowanych w proces przetwarzania informacji zostało przeprowadzone szkolenie z zakresu ochrony danych osobowych i bezpieczeństwa informacji[31].

8. Praca na odległość i mobilne przetwarzanie danych

Podstawa prawna:

- § 19 ust. 2 pkt 8 rozporządzenie KRI: Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez: ustanowienie podstawowych zasad gwarantujących bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość.

W UG w Branicach nie zostały ustanowione podstawowe zasady gwarantujące bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość, co zespół kontrolny stwierdza jako nieprawidłowość[32].

9. Serwis sprzętu informatycznego i oprogramowania

Podstawa prawna:

- § 19 ust. 2 pkt 10 rozporządzenie KRI: Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez: zawieranie w umowach serwisowych podpisanych ze stronami trzecimi zapisów gwarantujących odpowiedni poziom bezpieczeństwa informacji.

W przypadku systemów informatycznych niezbędnym jest objęcie ich (w zakresie oprogramowania użytkowego i systemowego, sprzętu oraz rozwiązań telekomunikacyjnych) stosownymi umowami serwisowymi, zapewniającymi zarówno szybkie uruchomienie pracy systemu w przypadku awarii, jak i bezpieczeństwo dla informacji uzyskanych przez wykonawców w związku z ich realizacją.

[31] Akta kontroli - Podpisana dokumentacja kontrolna: Szkolenie z zakresu ochrony danych osobowych i bezpieczeństwa informacji, str. 50-321

[32] Akta kontroli - Podpisana dokumentacja kontrolna: Polityka bezpieczeństwa danych osobowych wraz z załącznikami, str. 50-321, Akta kontroli - Protokół oględzin serwerowni, str. 332-335

W UG w Branicach wykorzystywane są trzy systemy teleinformatyczne przeznaczone do realizacji zadań zaleconych z zakresu administracji rządowej zakupione u zewnętrznego dostawcy.

W związku z powyższym zostały podpisane dwie umowy serwisowe. Jedna z nich z firmą Technika IT Sp. z o.o., do której dodatkowo zawarta została także umowa powierzenia przetwarzania danych osobowych[33]. Druga zawarta z MINFO – Usługi Komputerowe s.c., w której § 8 pkt 5 informuje, że Zleceniodawca powierza Zleceniobiorcy do przetwarzania dane osobowe. Wartym zauważenia jest fakt, iż w umowie zawartej z MINFO – Usługi Komputerowe s.c., nie zostały zawarte zapisy dot. czasu wykonania usługi oraz kar umownych za niewykonanie lub opóźnione wykonanie zadania[34]. Brak zawarcia w przedmiotowej umowie powyższych zapisów wiązać się może z brakiem zapewnienia ciągłości działania.

Biorąc powyższe pod uwagę, brak zapisów dot. czasu wykonania usługi oraz kar umownych za niewykonanie lub opóźnione wykonanie zadania, zespół kontrolny stwierdza jako nieprawidłowość.

10. Procedury zgłaszania incydentów naruszania BI

Podstawa prawna:

- § 19 ust. 2 pkt 13 rozporządzenie KRI: Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez: bezzwłoczne zgłaszanie incydentów naruszenia bezpieczeństwa informacji w określony i z góry ustalony sposób, umożliwiający szybkie podjęcie działań korygujących.

Zarówno w PBDO, jak i w żadnym z dokumentów stanowiących załączniki do PBDO, nie zostały określone procedury związane ze zgłaszaniem oraz reagowaniem w przypadku wystąpienia incydentów naruszenia bezpieczeństwa informacji[35].

Z analizy przedkontrolnej wynika, że w okresie objętym kontrolą nie miały miejsca przypadki wystąpienia incydentów naruszenia bezpieczeństwa informacji[36].

Brak procedur dot. reagowania na incydenty zostaje stwierdzone przez zespół kontrolny jako nieprawidłowość.

11. Audyt wewnętrzny z zakresu bezpieczeństwa informacji

Podstawa prawna:

[33] Akta kontroli - Podpisana dokumentacja kontrolna: Umowa o asystę techniczną, str. 50-321
[34] Akta kontroli - Podpisana dokumentacja kontrolna: Umowa MINFO, str. 50-321
[35] Akta kontroli - Podpisana dokumentacja kontrolna: Polityka bezpieczeństwa danych osobowych wraz z załącznikami, str. 50-321
[36] Akta kontroli - Ankieta dotycząca działania systemów teleinformatycznych, str. 14-18

- § 19 ust. 2 pkt 14 rozporządzenie KRI: Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez: zapewnienie okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji, nie rzadziej niż raz na rok.

Audyt bezpieczeństwa informacji jest działaniem mającym na celu zidentyfikowanie zagrożeń, które mogą powodować utratę poufności, integralności lub dostępności informacji. Celem przeprowadzenia audytu wewnętrznego bezpieczeństwa informacji jest ocena zakresu zgodności SZBI jednostki z kryteriami audytu.

W 2024 r. audyt z zakresu ochrony danych osobowych i bezpieczeństwa informacji[37] przeprowadzono w formie audytu wewnętrznego tylko w jednym z oddziałów UG w Branicach tj. w Referacie Organizacyjno-Prawnym.

W związku z brakiem przeprowadzania audytów KRI dla całego UG w Branicach, zespół kontrolny zwrócił się z złożenie wyjaśnień w tym zakresie. Wynika z nich, że „Przeprowadzenie w roku 2024 audytu KRI, wynikającego z § 19 ust. 2 pkt 14 Rozporządzenia Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych zaplanowane było na IV kwartał. W miesiącu wrześniu ubiegłego roku na terenie Gminy Branice wystąpiła powódź, która niestety dokonała znacznych zniszczeń na terenie gminy Branice. Znaczna część pracowników tut. Urzędu Gminy, w tym osoby odpowiedzialne za zlecenie audytu KRI, zaangażowana była w pracę zespołu zarządzania kryzysowego podczas klęski jak i podczas usuwania jej skutków z którymi jako gmina mierzymy się nadal. Dodatkowe obowiązki spowodowały niedopatrzenie polegające na braku zlecenia przeprowadzenia w/w audytu. (…).”[38]

Powyższe wyjaśnienia zostały przyjęte przez zespół kontrolny.

W związku z powyższym, zespół kontrolny zwrócił się o informację, kiedy – poza wskazanym audytem wewnętrznym z 2024 r. – w UG w Branicach został przeprowadzony ostatni audyt KRI, a także dokumentację potwierdzającą wykonanie ww. audytów. Wójt Gminy Branice złożył wyjaśnienia w powyższej kwestii o treści:

[37] Akta kontroli - Podpisana dokumentacja kontrolna: Audyt wewnętrzny, str. 50-321
[38] Akta kontroli - Pismo z wyjaśnieniami dot. pkt 3, str. 45

„W latach poprzednich Gmina nie zlecała firmom zewnętrznym przeprowadzenia audytu KRI”.[39]

Z § 19 ust. 2 pkt 14 rozporządzenie KRI wynika, że okresowe audyty wewnętrzne w zakresie bezpieczeństwa informacji winny być przeprowadzane nie rzadziej niż raz na rok. W związku z powyższym brak przeprowadzania audytów wewnętrznych w zakresie bezpieczeństwa informacji co najmniej raz na rok, zostaje stwierdzone jako nieprawidłowość.

12. Kopie zapasowe

Podstawa prawna:

- § 19 ust. 2 pkt 12 lit. b rozporządzenie KRI: Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez: zapewnienie odpowiedniego poziomu bezpieczeństwa w systemach teleinformatycznych, polegającego w szczególności na minimalizowaniu ryzyka utraty informacji w wyniku awarii.

Jednym z kluczowych sposobów zapobiegania utraty informacji w wyniku awarii jest wykonywanie kopii zapasowych. Takie działanie jest elementem planu ciągłości działania. Celem tworzenia kopii zapasowych jest możliwość odzyskania danych i przywrócenia do pracy użytkowej systemu teleinformatycznego wraz z informacjami przechowywanymi przez ten system, np. w bazie danych. Wymóg ten można osiągnąć poprzez przeprowadzanie regularnych kopii zapasowych całego środowiska pracy danego systemu teleinformatycznego, tj. systemu operacyjnego, jego konfiguracji (w tym konfiguracji zabezpieczeń), systemu informatycznego i informacji w nim przechowywanych.

W celu zapewnienia BI oraz systemów teleinformatycznych, w których informacje te są przetwarzane, w UG w Branicach sporządzone zostały procedury tworzenia kopii awaryjnych określone w § 5 i § 6 IZSI. Jednakże z analizy ich zapisów wynika, że przedmiotowe wytyczne nie są na bieżąco aktualizowane, co zespół kontrolny stwierdza jako uchybienie.

W związku z powyższym, kontrolujący rekomendują, aby w celu zwiększenia bezpieczeństwa informacji oraz zminimalizowaniu ryzyka utraty przetwarzanych informacji w wyniku awarii, w UG w Branicach zostały opracowane i wdrożone szczegółowe procedury uwzględniające, m.in:

- wykonywanie kopii zapasowych zgodnie z ustalonym harmonogramem;
- przywracanie danych z kopii wraz z opisaniem procedur weryfikacji;

[39] Akta kontroli - Wyjaśnienia dot. kontroli wraz z podpisaną dokumentacją: wyjaśnienia dot. pkt 4, str. 326-330

- poprawności wykonania i przywracania kopii;
- wykonywanie kopii zapasowych poza system informatyczny przechowywanie kopii zapasowych poza siedzą urzędu.

Z informacji uzyskanych od Wójta Gminy Branice w UG w Branicach wykonywane są kopie zapasowe za pomocą [redacted][40].

13. Projektowanie, wdrażanie i eksploatacja systemów teleinformatycznych

Podstawa prawna:

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

W UG w Branicach do realizacji zadań z zakresu administracji rządowej wykorzystywane są wspomagające systemy teleinformatyczne, które dzielą się na systemy centralne oraz lokalne (zakupione u dostawcy zewnętrznego).
Na obsługę zakupionych systemów informatycznych zawarte zostały stosowne umowy licencyjne, gwarantująca rozwój i dostosowanie do obowiązujących przepisów prawa. Przedmiotowe systemy teleinformatyczne zostały zaprojektowane, wdrożone i eksploatowane z uwzględnieniem ich funkcjonalności, niezawodności, używalności, wydajności, przenoszalności i pielęgnowalności.

14. Zabezpieczenia techniczno-organizacyjne dostępu do informacji

Podstawa prawna:

- § 19 ust. 2 rozporządzenie KRI: Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez:
  pkt 7 - zapewnienie ochrony przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami, przez: a) monitorowanie dostępu do informacji, b) czynności zmierzające do wykrycia nieautoryzowanych działań związanych z przetwarzaniem informacji,
  c) zapewnienie środków uniemożliwiających nieautoryzowany dostęp na poziomie systemów operacyjnych, usług sieciowych i aplikacji;
  pkt 9 - zabezpieczenie informacji w sposób uniemożliwiający nieuprawnionemu jej ujawnienie, modyfikacje, usunięcie lub zniszczenie;

[40] Akta kontroli - Wyjaśnienia dot. kontroli wraz z podpisaną dokumentacją: wyjaśnienia dot. pkt 2, str. 326-330

pkt 11 - ustalenie zasad postępowania z informacjami, zapewniającymi minimalizację wystąpienia ryzyka kradzieży informacji i środków przetwarzania informacji, w tym urządzeń mobilnych.

W celu uzyskania odpowiedniego poziomu BI przy jednoczesnym zapewnieniu właściwego do nich dostępu przez uprawnionych użytkowników stosowany jest szereg zabezpieczeń informatycznych. Celem takich zabezpieczeń jest uzyskanie ochrony przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami, a także np. kradzieżą środków przetwarzania informacji.

W PBDO, IZSI oraz Regulaminie Pracy Urzędu Gminy w Branicach[41] zostały określone wytyczne dot. zabezpieczeń dostępu do informacji.

W trakcie wizji lokalnej zespół kontrolny stwierdził, że wybrani pracownicy po zakończonej pracy zabierają klucze do pomieszczeń ze sobą. W związku z powyższym, zwrócono się o złożenie wyjaśnień w przedmiotowym zakresie. Wynika z nich, że w UG w Branicach zostało wydane Zarządzenie nr 114U/24 Wójta Gminy Branice z dnia 20 grudnia 2024 r. w sprawie upoważnienia pracowników do dostępu do systemu alarmowego budynku Urzędu Gminy Branice oraz do zabezpieczenia budynku i miejsca pracy po zakończonej pracy, które upoważnia określonych pracowników UG w Branicach do wynoszenia kluczy do pomieszczeń oraz do otwierania i zamykania budynku Urzędu wraz z dostępem do systemu alarmowego[42].

W związku z informacjami powziętymi podczas wizji lokalnej przeprowadzonej w UG w Branicach oraz zapisami w dokumentacji sporządzonej po przeprowadzeniu analizy ryzyka, z której wynika, że propozycją dot. zastosowania środków zaradczych jest szyfrowanie dysków, zwrócono się o złożenie wyjaśnień dot. braku ich szyfrowania w laptopach. Z wyjaśnień wynika, że „w celu zabezpieczenia urządzeń stosowano loginy i hasła do systemu operacyjnego jak i użytkowanych programów”. Brak szyfrowania dysków twardych zostaje stwierdzone jako uchybienie[43].

Dodatkowo w trakcie wizji lokalnej, zespół kontrolny zauważył, że proces drukowania na drukarkach ogólnodostępnych znajdujących na korytarzach UG w Branicach nie jest zabezpieczony, np. kodem PIN. W związku z powyższym

[41] Stanowi załącznik do Zarządzenia Nr 2U/24 Wójta Gminy Branice z dnia 17 stycznia 2024 r. w sprawie wprowadzenia Regulaminu Pracy w Urzędzie Gminy w Branicach
[42] Akta kontroli - Pismo z wyjaśnieniami dot. pkt 1, str. 43, Akta kontroli - Pismo z wyjaśnieniami dot. pkt 2, str. 44
[43] Akta kontroli - Pismo z wyjaśnieniami dot. pkt 4, str. 46

zwrócono się o złożenie wyjaśnień, z których wynika, że „Pracownicy Urzędu Gminy po wydrukowaniu dokumentów na drukarkach znajdujących się na korytarzach budynku Urzędu Gminy na bieżąco zabierają wydrukowane materiały z urządzeń. Dodatkowo większość pracowników wyposażonych jest w urządzenia drukujące znajdujące się w danym biurze na których wykonywane są wydruki dokumentów. W celu zwiększenia bezpieczeństwa ochrony danych rozpoczęliśmy wdrażanie systemu zaszyfrowanego dostępu do udostępnionych na korytarzach drukarek.” [44]

Zespół kontrolny przyjął powyższe wyjaśnienia, jednakże kontrolujący rekomendują w przyszłości podjęcie działań mających na celu zwiększenie bezpieczeństwa informacji oraz danych przetwarzanych przez UG w Branicach. W przypadku ewentualnej zmiany miejsca lokalizacji drukarek należy mieć na względzie również prawidłowe zabezpieczenie gniazdek sieciowych znajdujących się na korytarzach.

15. Zabezpieczenia techniczno-organizacyjne systemów informatycznych

Podstawa prawna:

- § 19 ust. 2 pkt 12 rozporządzenie KRI: Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez: zapewnienie odpowiedniego poziomu bezpieczeństwa w systemach teleinformatycznych, polegającego w szczególności na: a) dbałości o aktualizację oprogramowania, b) minimalizowaniu ryzyka utraty informacji w wyniku awarii, c) ochronie przed błędami, utratą, nieuprawnioną modyfikacją, d) stosowaniu mechanizmów kryptograficznych w sposób adekwatny do zagrożeń lub wymogów przepisu prawa, e) zapewnieniu bezpieczeństwa plików systemowych, f) redukcji ryzyk wynikających z wykorzystania opublikowanych podatności technicznych systemów teleinformatycznych, g) niezwłocznym podejmowaniu działań po dostrzeżeniu nieujawnionych podatności systemów teleinformatycznych na możliwość naruszenia bezpieczeństwa, h) kontroli zgodności systemów teleinformatycznych z odpowiednimi normami i politykami bezpieczeństwa.

Poza Zabezpieczeniami techniczno-organizacyjnymi dostępu do informacji, w PBDO oraz IZSI zostały określone także zabezpieczenia dla systemów informatycznych.

Dodatkowo zapewniono także środki uniemożliwiające nieautoryzowany dostęp oraz zapewniające kontrolę dostępu do systemów teleinformatycznych służących

[44] Akta kontroli - Pismo z wyjaśnieniami dot. pkt 7, str. 49

do realizacji zadań zleconych z zakresu administracji rządowej poprzez indywidualne logowanie do wybranych systemów[45].

Podczas kontroli dokonano oględzin pomieszczenia serwerowni w UG w Branicach. Czynność ta została przeprowadzona w obecności Pracownika na stanowisku ds. informatyki i obsługi urzędowych stron internetowych oraz IOD[46]. W związku z powyższym celem zapewnienia nie tylko odpowiedniego poziomu bezpieczeństwa informacji oraz zminimalizowania ryzyka nieautoryzowanego dostępu i potencjalnych zagrożeń, ale przede wszystkim, chroniąc życie i zdrowie pracowników Urzędu, zespół kontrolny rekomenduje, aby serwerownia poza zabezpieczeniami stosowanymi obecnie, stanowiła odrębne pomieszczenie, zabezpieczone wzmocnionymi drzwiami wraz z ewidencją wejść i wyjść do serwerowni.

16. Rozliczalność działań w systemach teleinformatycznych

Podstawa prawna:

- § 20 ust. 2 rozporządzenie KRI: W dziennikach systemów odnotowuje się obligatoryjnie działania użytkowników lub obiektów systemowych polegające na dostępie do: 1) systemu z uprawnieniami administracyjnymi; 2) konfiguracji systemu, w tym konfiguracji zabezpieczeń; 3) przetwarzanych w systemach danych podlegających prawnej ochronie w zakresie wymaganym przepisami prawa;
- § 20 ust. 3 rozporządzenie KRI: Poza informacjami wymienionymi w ust. 2 mogą być odnotowywane działania użytkowników lub obiektów systemowych, a także inne zdarzenia związane z eksploatacją systemu w postaci: 1) działań użytkowników nieposiadających uprawnień administracyjnych, 2) zdarzeń systemowych nieposiadających krytycznego znaczenia dla funkcjonowania systemu, 3) zdarzeń i parametrów środowiska, w którym eksploatowany jest system teleinformatyczny - w zakresie wynikającym z analizy ryzyka;
- § 20 ust. 4 rozporządzenie KRI: Informacje w dziennikach systemów przechowywane są od dnia ich zapisu, przez okres wskazany w przepisach odrębnych, a w przypadku braku przepisów odrębnych przez dwa lata.

[45] Akta kontroli - Podpisana dokumentacja kontrolna: Oprogramowanie używane w Urzędzie Gminy Branice, wykaz osób z dostępem i sposobem logowania, str. 50-321
[46] Akta kontroli - Protokół oględzin serwerowni, str. 332-335

Z dokumentacji oraz informacji uzyskanych w trakcie kontroli wynika, że UG w Branicach odnotowuje obligatoryjne działania użytkowników w dziennikach systemów[47].

Dodatkowo, z wyjaśnień Wójta Gminy Branice wynika, że „Informacje w dziennikach systemów przechowywane są od dnia ich zapisu przez okres wymagany w przepisach i archiwizowane łącznie z bazami programów objętych kontrolą."[48].

III. Zakres, przyczyny i skutki stwierdzonych nieprawidłowości oraz osoby odpowiedzialne za nieprawidłowości

W wyniku kontroli stwierdzono następujące nieprawidłowości:

1. Brak opracowania, ustanowienia, wdrożenia i eksploatowania, monitorowania i przeglądania oraz utrzymania i doskonalenia Systemu Zarządzania Bezpieczeństwem Informacji, co narusza § 19 ust. 1 i 2 rozporządzenia KRI;
2. Brak przeprowadzania przeglądów zarządzenia w sprawie wprowadzenia „Polityki bezpieczeństwa danych osobowych Urzędu Gminy w Branicach" wraz z jego załącznikami, co narusza § 19 ust. 2 pkt 1 rozporządzenia KRI;
3. Brak ustanowienia podstawowych zasad gwarantujących bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość, co narusza § 19 ust. 2 pkt 8 rozporządzenia KRI;
4. Brak zapisów w umowie serwisowej dot. czasu wykonania usługi oraz kar umownych za niewykonanie lub opóźnione wykonanie zadania, co narusza § 19 ust. 2 pkt 10 rozporządzenia KRI;
5. Brak procedur dot. reagowania na incydenty, co narusza § 19 ust. 2 pkt 13 rozporządzenia KRI;
6. Brak przeprowadzania audytów bezpieczeństwa informacji, nie rzadziej niż raz na roku, co narusza § 19 ust. 2 pkt 14 rozporządzenia KRI.

Dodatkowo w wyniku kontroli zostały stwierdzone poniższe uchybienia:

1. Składanie w formie ustnej wniosków o nadanie/zmianę/cofnięcie uprawnień dostępu do systemów;

[47] Akta kontroli - Podpisana dokumentacja kontrolna: Dzienniki zdarzeń z programów Podatki i JGU, str. 50-321
[48] Akta kontroli - Wyjaśnienia dot. kontroli wraz z podpisaną dokumentacją: wyjaśnienia dot. pkt 3, str. 326-330

2. Brak aktualizacji procedury tworzenia kopii awaryjnych określonych w § 5 i § 6 IZSI;
3. Brak szyfrowania dysków twardych w użytkowanych laptopach.

IV. Informacje o zastrzeżeniach zgłoszonych do projektu wystąpienia pokontrolnego i wyniku ich rozpatrzenia lub o niezgłoszeniu zastrzeżeń

Kierownik jednostki kontrolowanej pismem z dnia 28 sierpnia 2025 r. znak: SK.1710.3.2025.KH zgłosił zastrzeżenia do projektu wystąpienia pokontrolnego, które pismem z dnia 09 października 2025 r. znak PN.I.431.4.3.2025.NL zostały oddalone w całości.

V. Zalecenia lub wnioski dotyczące usunięcia nieprawidłowości lub usprawnienia funkcjonowania jednostki kontrolowanej

W związku z ustaleniami dokonanymi podczas kontroli zalecam:

1. Opracować, ustanowić, wdrożyć i eksploatować, monitorować i przeglądać oraz utrzymywać i doskonalić System Zarządzania Bezpieczeństwem Informacji;
2. Przeprowadzać przeglądy zarządzenia w sprawie wprowadzenia „Polityki bezpieczeństwa danych osobowych Urzędu Gminy w Branicach” wraz z jego załącznikami;
3. Ustanowić podstawowe zasady gwarantujące bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość;
4. Zawierać w umowach serwisowych zapisy dot. czasu wykonania usługi oraz kar umownych za niewykonanie lub opóźnione wykonanie zadania;
5. Sporządzić wytyczne dot. reagowania na incydenty;
6. Przeprowadzać, nie rzadziej niż raz na rok, audyt bezpieczeństwa informacji;
7. Wnioski o nadanie/zmianę/cofnięcie uprawnień dostępu do systemów składać w formie pisemnej;
8. Zaktualizować procedurę tworzenia kopii awaryjnych;
9. Szyfrować dyski twarde w laptopach użytkowanych w UG w Branicach.

VI. Ocena wskazująca na niezasadność zajmowania stanowiska lub pełnienia funkcji przez osobę odpowiedzialną za stwierdzone nieprawidłowości:

nie dotyczy.

VII. **Na podstawie art. 49 oraz art. 46 ust. 3 pkt 3 ustawy z dnia 15 lipca 2011 r. o kontroli w administracji rządowej (t.j. Dz.U. z 2020 r. poz. 224), proszę o przekazanie pisemnej informacji o sposobie wykonania zaleceń, wykorzystaniu wniosków lub przyczynach ich niewykorzystania, o podjętych działaniach lub przyczynach ich niepodjęcia, albo o innym sposobie usunięcia stwierdzonych nieprawidłowości, w terminie 90 dni od dnia otrzymania niniejszego dokumentu.**

VIII. **Zgodnie z art. 48 ustawy o kontroli, od wystąpienia pokontrolnego nie przysługują środki odwoławcze.**

Z up. Wojewody Opolskiego

Katarzyna Piasecka
kierownik
Wydział Prawny i Nadzoru

Pismo zostało wydane w postaci elektronicznej i podpisane kwalifikowanym podpisem elektronicznym