Kontrole z zakresu działania systemów teleinformatycznych używanych do realizacji zadań zleconych z zakresu administracji rządowej oraz bezpieczeństwa teleinformatycznego w administracji rządowej i ochrony danych osobowych –2024 r.

Podstawa prawna do przeprowadzenia kontroli:
- art. 25 ust. 1 pkt 3 lit. a w związku z ust. 3 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne[1];
- art. 28 ust. 1 pkt 1 ustawy z dnia 23 stycznia 2009 r. o wojewodzie i administracji rządowej w województwie.[2]

Przedmiot kontroli:
- **Działanie systemów teleinformatycznych używanych do realizacji zadań zleconych z zakresu administracji rządowej;**
- **Bezpieczeństwo teleinformatyczne w administracji rządowej i ochrona danych osobowych.**

Łączna liczba przeprowadzonych kontroli: **6**

Jednostki kontrolowane: Urząd Miasta i Gminy w Człopie, Urząd Miejski w Dobrzanach, Urząd Miejski w Chociwlu, Urząd Gminy Kozielice, Urząd Gminy Świeszyno, Komenda Wojewódzka Państwowej Straży Pożarnej w Szczecinie.

Liczba kontroli, w których stwierdzono nieprawidłowości: 5

Zakres stwierdzonych nieprawidłowości:
- Nieprzeglądanie i nieaktualizowanie obowiązującej w Urzędzie dokumentacji dotyczącej bezpieczeństwa informacji;
- Nieprzeprowadzenie audytu wewnętrznego z zakresu bezpieczeństwa informacji;
- Nieprzeprowadzenie okresowo analizy ryzyka utraty integralności, dostępności lub poufności informacji;
- Dokumentacja regulująca kwestie bezpieczeństwa informacji nie zawiera wszystkich elementów wymaganych przepisami rozporządzenia KRI;
- Zakres tematyczny szkoleń przeprowadzonych w Urzędzie nie obejmował wszystkich zagadnień wskazanych w § 19 ust. 2 pkt 6 rozporządzenia KRI;
- Realizowanie audytów wewnętrznych przez osobę pełniącą równocześnie funkcję IOD i ASI, w konsekwencji czego dokonywanie oceny własnej działalności w odniesieniu do rozporządzenia KRI i RODO;
- Nieuwzględnienie zabezpieczeń ochrony kryptograficznej w procedurach określających zasady gwarantujące bezpieczną pracę przy przetwarzaniu mobilnym i w przypadku świadczenia pracy na odległość;
- W umowie regulującej kwestię serwisu programu podlegającego kontroli brak zapisów określających maksymalny czas skutecznej naprawy oprogramowania;
- Zawężenie incydentów naruszenia bezpieczeństwa informacji do naruszeń danych osobowych;

[1] Dz. U. z 2023 r., poz. 57.
[2] Dz. U. z 2023 r., poz. 190.

- Zawężenie analizy ryzyka do zagadnień związanych z bezpieczeństwem danych osobowych;
- Nieprzechowywanie logów programu podlegających kontroli przez okres 2 lat;
- Nieprzeprowadzanie testowych odtworzeń kopii zapasowych na potrzeby weryfikacji poprawności i stanu ich wykonywania;
- Nieprowadzenie działań związanych z przeglądaniem logów i ich analizą w celu identyfikacji działań niepożądanych;
- Niesporządzanie dokumentacji dotyczącej testowania kopii zapasowych danych i systemów na potrzeby weryfikacji poprawności i stanu ich wykonywania oraz dokumentacji działań związanych z przeglądaniem logów systemowych;
- Nieprowadzenie rejestru wejść osób spoza Urzędu do pomieszczenia serwerowni;
- Pomieszczenie serwerowni nie jest wyposażone we wszystkie wymagane zabezpieczenia chroniące przed nieuprawnionym dostępem, uszkodzeniem lub zniszczeniem infrastruktury IT.