Ministerstwo
Spraw Wewnętrznych
i Administracji
Departament Kontroli

Warszawa, dnia 26 maja 2022 r.

Informacja o wynikach kontroli
na temat: *Działanie systemów teleinformatycznych używanych do realizacji zadań publicznych albo realizacji obowiązków wynikających z art. 13 ust. 2 ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne* w Śląskim Urzędzie Wojewódzkim w Katowicach.

I. Podstawa prawna

Czynności kontrolne zostały przeprowadzone na podstawie ustawy z dnia 15 lipca 2011 r. *o kontroli w administracji rządowej*[1].

II. Tryb kontroli

Kontrola została przeprowadzona przez Departament Kontroli Ministerstwa Spraw Wewnętrznych i Administracji w trybie zwykłym, zgodnie z *Planem kontroli Ministerstwa Spraw Wewnętrznych i Administracji na rok 2021.*

III. Termin kontroli

Od 13 grudnia 2021 r. do 27 stycznia 2022 r.

IV. Zakres kontroli obejmował następujące zagadnienia:

1) Wymiana informacji w postaci elektronicznej, w tym współpraca z innymi systemami/rejestrami informatycznymi i wspomaganie świadczenia usług drogą elektroniczną.
2) Zarządzanie bezpieczeństwem informacji w systemach teleinformatycznych.

V. Kontrolą objęto okres od 1 stycznia 2020 r. do 30 listopada 2021 r.[2]

VI. Ustalenia kontroli – ocena kontrolowanej działalności

Pozytywnie oceniono obszar wymiany informacji w postaci elektronicznej, w tym współpracy z innymi systemami/rejestrami informatycznymi i wspomaganie świadczenia usług drogą elektroniczną. Śląski Urząd Wojewódzki w Katowicach udostępniał elektroniczną skrzynkę podawczą pozwalającą na przesyłanie drogą elektroniczną pism kierowanych do Urzędu, a także zapewnił możliwość elektronicznej rejestracji wizyt oraz elektronicznej formy kontaktu w sprawach bieżących za pośrednictwem formularza kontaktowego. Podstawowym sposobem dokumentowania przebiegu załatwiania i rozstrzygania spraw oraz wykonywania czynności kancelaryjnych w Urzędzie był system do elektronicznego zarządzania dokumentacją EZD.

[1] t.j. Dz. U. z 2020 r. poz. 224.
[2] Badaniami kontrolnymi objęto również zdarzenia i dokumenty sprzed 1 stycznia 2020 r. i po 30 listopada 2021 r. w przypadkach, gdy miały one wpływ lub miały związek z zagadnieniami będącymi przedmiotem kontroli, a ich wyłączenie z kontroli nie pozwoliłoby na ocenę kontrolowanej działalności. W obszarze związanym z projektowaniem, wdrażaniem i funkcjonowaniem systemów teleinformatycznych kontrolą objęto okres od dnia rozpoczęcia prac projektowych, zaś w zakresie umów serwisowych okres od dnia zawarcia badanej umowy.

W kontrolowanym okresie w Śląskim Urzędzie Wojewódzkim w Katowicach funkcjonował System Zarządzania Bezpieczeństwem Informacji[3] wprowadzony na mocy zarządzenia Nr 423/16 Wojewody Śląskiego z dnia 21 grudnia 2016 r. System ten regulował kluczowe dla zarządzania bezpieczeństwem informacji obszary w celu zapewnienia poufności, dostępności i integralności informacji. W jednostce stosowano zabezpieczenia techniczne i organizacyjne dostępu do informacji i systemów teleinformatycznych, zapewniono inwentaryzację sprzętu i oprogramowania informatycznego oraz rozliczalność działań użytkowników w systemach teleinformatycznych. Jednostka określiła sposób zarządzania incydentami bezpieczeństwa informacji, zasady minimalizujące ryzyka utraty informacji w wyniku awarii, zasady zarządzania uprawnieniami do pracy w systemach i zasady bezpiecznej pracy na odległość. Urząd aktywnie podejmował działania w obszarze podnoszenia świadomości pracowników zaangażowanych w proces przetwarzania informacji, m.in. uruchomił e-learningową Platformę Szkoleniową oraz zapewnił szkolenia specjalistyczne z zakresu bezpieczeństwa informacji.

Za **nieprawidłowość** uznano niezapewnienie formalnego wymogu zatwierdzenia przez Kierownictwo Śląskiego Urzędu Wojewódzkiego zmian w dokumentacji SZBI i wynikającą z powyższego niemożność potwierdzenia zaangażowania Kierownictwa w proces doskonalenia SZBI oraz nieodzwierciedlanie w dokumentacji SZBI, w sposób przejrzysty i uporządkowany, zmian zachodzących w jej obrębie. W Urzędzie dokonywano bowiem aktualizacji dokumentacji tworzącej SZBI, w tym dostosowania do zmian w obszarze ochrony danych osobowych związanych z wejściem w życie RODO[4] i ustawy z dnia 10 maja 2018 r. *o ochronie danych osobowych*[5], niemniej zmiany wprowadzono bezpośrednio w intranecie, bez właściwej formy ich dokumentowania i zatwierdzania. Ponadto, za uchybienie uznano niepoinformowanie pracowników przez Kierownictwo Śląskiego Urzędu Wojewódzkiego o zmianach wprowadzonych w SZBI, w związku z wejściem w życie RODO. Informacja o nowych wzorach dokumentów została bowiem przekazana wyłącznie przez inspektora ochrony danych[6].

Zespół Audytu Wewnętrznego Śląskiego Urzędu Wojewódzkiego realizował okresowe audyty bezpieczeństwa informacji, w których wskazywał obszary wymagające zmian lub doskonalenia oraz monitorował ich wykonanie. Wykonane w październiku 2018 r. przez komórkę audytu wewnętrznego czynności doradcze w obszarze bezpieczeństwa informacji wpłynęły na podjęcie przez Kierownictwo Śląskiego Urzędu Wojewódzkiego decyzji o potrzebie przebudowy systemu. W kontrolowanym okresie Urząd pracował nad wprowadzeniem nowych regulacji SZBI, niemniej przedłużający się czas wprowadzenia zalecanych przez audyt wewnętrzny zmian uznano za uchybienie.

Jednocześnie za **nieprawidłowość** uznano nieprzeprowadzenie, w czasie przedłużających się prac nad nową dokumentacją SZBI, formalnego przeglądu funkcjonujących rozwiązań pod kątem wprowadzenia pilnych zmian doskonalących i dostosowujących regulację do zmieniającego się otoczenia oraz niedokonanie formalnej zmiany w obszarze pełnionej przez inspektora ochrony danych roli w procesie aktualizacji SZBI. Przedłużający się czas wdrożenia nowego SZBI, przy jednoczesnym braku okresowego przeglądu funkcjonującego systemu i dokonywania w nim zmian, spowodował, że jednostka kontrolowana przez okres ponad 3 lat funkcjonowała w oparciu o dokumentację nie w pełni dostosowaną do zmieniającego się otoczenia i swoich potrzeb.

Ponadto za **nieprawidłowość** uznano:

- ponad siedmiomiesięczne opóźnienie w realizacji obowiązku zawiadomienia Prezesa Urzędu Ochrony Danych Osobowych[7] o wyznaczeniu inspektora ochrony danych,

[3] Zwany dalej: SZBI.

[4] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. *w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE* (ogólne rozporządzenie o ochronie danych) - Dz. U. UE. L. z 2016 r. Nr 119, str. 1 z późn. zm. – dalej jako: RODO.

[5] T.j. Dz. U. z 2019 r., poz. 1781.

[6] Dalej przywoływany jako: IOD.

[7] Dalej przywoływany jako: Prezes UODO.

- niezatwierdzanie przez Kierownictwo Śląskiego Urzędu Wojewódzkiego dokumentu pn. *Sprawozdanie podsumowujące wyniki szacowania ryzyk informatycznych* pełniącego funkcję planu postępowania z ryzykiem informatycznym w Śląskiego Urzędu Wojewódzkiego,
- ponad pięciomiesięczne opóźnienie w odebraniu uprawnień dostępu do poczty elektronicznej byłemu pracownikowi,
- blisko dwumiesięczne opóźnienie w podpisaniu umowy na opiekę autorską i usługę serwisową Systemu Kolejkowego,
- przechowywanie kopii zapasowych systemów wirtualnych w tej samej lokalizacji co zabezpieczane systemy,
- brak regulacji wewnętrznych w zakresie projektowania i wdrażania systemów teleinformatycznych,
- niedostosowanie *Procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych* w zakresie planowania przeglądów systemów informatycznych i raportowania ich wyników do zmian związanych z wejściem w życie przepisów RODO i rzeczywiście podejmowanych działań.

VII. Wnioski i zalecenia pokontrolne

W celu wyeliminowania ze służbowej działalności stwierdzonych w trakcie kontroli nieprawidłowości i uchybień oraz usprawnienia funkcjonowania kontrolowanej jednostki zalecono:

1. Zapewnienie, aby wprowadzony w dniu 28 marca 2022 r. System Zarządzania Bezpieczeństwem Informacji gwarantował:
   - zaangażowanie kierownictwa Śląskiego Urzędu Wojewódzkiego w proces doskonalenia SZBI, w szczególności poprzez formalne zatwierdzanie zmian w dokumentacji SZBI oraz informowanie pracowników o wprowadzanych zmianach,
   - przeprowadzanie udokumentowanych okresowych przeglądów SZBI,
   - doradczą rolę inspektora ochrony danych w opracowywaniu i aktualizowaniu SZBI,
   - zatwierdzanie przez Kierownictwo Śląskiego Urzędu Wojewódzkiego planu postępowania z ryzykiem informatycznym,
   - bezzwłoczne odbieranie byłym pracownikom uprawnień dostępowych do systemów teleinformatycznych,
   - uregulowanie kwestii związanych z koniecznością zapewniania bezpieczeństwa w fazie projektowania i wdrażania systemów teleinformatycznych,
   - dostosowanie procedur wykonywania przeglądów i konserwacji systemów informatycznych, do rzeczywiście podejmowanych działań.
2. Systematyczne dokonywanie aktualizacji dokumentacji SZBI w zakresie dotyczącym zmieniającego się otoczenia oraz bieżące monitorowanie i doskonalenie Systemu Zarządzania Bezpieczeństwem Informacji.
3. Zapewnienie ciągłości umów na opiekę autorską i usługi serwisowe systemów teleinformatycznych Śląskiego Urzędu Wojewódzkiego.
4. Kontynuowanie prac związanych z uruchomieniem serwerowni zapasowej znajdującej w innej lokalizacji niż zabezpieczane systemy.
5. Przestrzeganie określonego w art. 10 ust. 1 ustawy *o ochronie danych osobowych* terminu na zawiadamianie Prezesa Urzędu Danych Osobowych o wyznaczeniu/zmianie inspektora ochrony danych lub jego zastępcy.