NAJWYŻSZA IZBA KONTROLI

KAP.430.9.2024
Nr ewid. 123/2024/P/24/004/KAP

Informacja o wynikach kontroli

ZAPEWNIENIE BEZPIECZEŃSTWA INFORMACJI ORAZ CIĄGŁOŚCI DZIAŁANIA SYSTEMÓW INFORMATYCZNYCH W JEDNOSTKACH SAMORZĄDU TERYTORIALNEGO

MISJĄ

Najwyższej Izby Kontroli jest niezależna, profesjonalna kontrola zadań publicznych w interesie obywateli i państwa

p.o. Dyrektor Departamentu
Administracji Publicznej

Bogdan Skwarka
/podpisano elektronicznie/

Wiceprezes Najwyższej Izby Kontroli

Jacek Kozłowski
/podpisano elektronicznie/

Prezes Najwyższej Izby Kontroli

Marian Banaś
/podpisano elektronicznie/

Warszawa, luty 2025

Najwyższa Izba Kontroli
ul. Filtrowa 57
02-056 Warszawa
+48 22 444 50 00
nik@nik.gov.pl
www.nik.gov.pl

SPIS TREŚCI

WYKAZ SKRÓTÓW, SKRÓTOWCÓW I POJĘĆ

administrator	zgodnie z definicją zawartą w RODO, oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych (art. 4 pkt 7 RODO);
administrator systemów informatycznych (ASI)	odpowiada za zarządzanie systemami informatycznymi w tym systemami wykorzystywanymi w procesie przetwarzania danych osobowych. W zakresie przetwarzania danych osobowych współpracuje z Inspektorem ochrony danych;
aktywa informacyjne	zidentyfikowane zbiory danych urzędu;
aktywa informatyczne	oprogramowanie, dane, sprzęt, dokumentacja, zasoby administracyjne fizyczne, komunikacyjne lub ludzkie związane z działalnością informatyczną;
ciągłość działania	strategiczna i taktyczna zdolność organizacji do przewidywania i reagowania na zdarzenia kryzysowe, które mogą prowadzić do zakłóceń działalności. W tym celu opracowywany jest plan ciągłości działania, który ma za zadanie przygotować organizację na wypadek wystąpienia zdarzeń kryzysowych, aby tam, gdzie to możliwe, szybko przywrócić normalne warunki, a tam, gdzie to niemożliwe, przejść do zaplanowanego sposobu zastępczego wykonywania zadań;
dane osobowe	informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą"); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden, bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej (art. 4 pkt 1 RODO);
incydent	pojedyncze zdarzenie lub seria niepożądanych lub niespodziewanych zdarzeń związanych z bezpieczeństwem informacji, które stwarzają prawdopodobieństwo zakłócenia działań i zagrażają zachowaniu bezpieczeństwa informacji;
integralność danych	właściwość polegająca na tym, iż dane nie podlegają nieautoryzowanym zmianom, w tym przypadkowej lub celowej modyfikacji, fałszowaniu czy usunięciu;
IOD – inspektor ochrony danych	wyznaczany w związku z art. 37 RODO; zasadniczą rolą inspektorów ochrony danych jest doradzanie i weryfikacja prawidłowości wykonywania obowiązków wynikających z przepisów prawa dotyczących przetwarzania danych osobowych. Rola ta nie oznacza przeniesienia na IOD odpowiedzialności za zgodne z prawem przetwarzanie danych osobowych, ponieważ nadal to administrator danych będzie ponosił pełną odpowiedzialność za zgodne z prawem przetwarzanie danych osobowych. Dlatego w interesie kierownictwa każdego podmiotu publicznego jest mieć niezależnego, właściwie usytuowanego w strukturze organizacyjnej, inspektora ochrony danych, który będzie mógł efektywnie realizować swoje obowiązki;
jst	Jednostka samorządu terytorialnego;

plan zapewnienia ciągłości działania	ma za zadanie przygotować organizację na wypadek zdarzeń nadzwyczajnych (np. wojna, pandemia, atak hackerski, katastrofa budowlana czy katastrofy jak pożar, zalanie, brak prądu czy powódź). Plan taki powinien zawierać procedury działania, które umożliwią sprawną komunikację i ciągłość jego działania, a co za tym idzie zminimalizują ryzyko wystąpienia chaosu i dezinformacji oraz ograniczą negatywne konsekwencje wiążące się z danym zdarzeniem;
podatność	właściwość systemu informatycznego, która może być wykorzystana przez zagrożenie cyberbezpieczeństwa;
podmiot przetwarzający	osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który przetwarza dane osobowe w imieniu administratora (art. 4 pkt 8 RODO);
polityka bezpieczeństwa informacji (PBI)	zbiór reguł i procedur określających organizację i zarządzanie bezpieczeństwem informacji w jednostce;
przetwarzanie	operacja lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taka jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie (art. 4 pkt 2 RODO);
RODO	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)[1];
wcześniejsze rozporządzenie KRI	rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych[2]. Obowiązywało do 22 maja 2024 r.;
obowiązujące rozporządzenie KRI	rozporządzenie 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[3]. Obowiązuje od 23 maja 2024 r.;
ryzyko	potencjalne zdarzenie i jego konsekwencje, oszacowane pod względem wagi oddziaływania i prawdopodobieństwa wystąpienia;
ryzyko związane z bezpieczeństwem informacji	potencjalna sytuacja, w której określone zagrożenie wykorzysta podatność aktywów lub grupy aktywów powodując w ten sposób szkodę dla organizacji. Ryzyko mierzone jest jako kombinacja prawdopodobieństwa zdarzenia i jego następstw;

[1] Dz. Urz.UE.L 119 z 04.05.2016, str. 1, ze zm.

[2] Dz. U. z 2017 r. poz. 2247.

[3] Dz. U. poz. 773.

skuteczność działań	realizacja wyznaczonych celów. Oznacza zakres w jakim program lub jednostka realizuje swoje cele i założenia[4];
System Zarządzania Bezpieczeństwem Informacji (SZBI)	cześć całościowego systemu zarządzania, oparta na podejściu wynikającym ze zidentyfikowanego ryzyka biznesowego, odnosząca się do ustanawiania, wdrażania, eksploatacji, monitorowania, utrzymywania i doskonalenia bezpieczeństwa informacji;
ustawa o informatyzacji	ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne[5];
ustawa o ksc	ustawa z dnia 5 lipca 2018 r. o Krajowym Systemie Cyberbezpieczeństwa[6];
ustawa o NIK	ustawa z dnia 23 grudnia 1994 r. o Najwyższej Izbie Kontroli[7];
współdzielenie informacji	wspólne użytkowanie tych samych zasobów informacyjnych przez różne osoby, podmioty lub procesy;
zagrożenie bezpieczeństwa informacji	potencjalna przyczyna wystąpienia incydentu;
zarządzanie ryzykiem	skoordynowane działania mające na celu kierowanie organizacją i kontrolowanie organizacji pod względem ryzyka;
zbiór danych	uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie (art. 4 pkt 6 RODO).

4 Standardy i wytyczne kontroli wykonania zadań na podstawie standardów kontroli INTOSAI i praktyki.

5 Dz. U. z 2024 r. poz. 1557, ze zm.

6 Dz. U. z 2024 r. poz. 1077, ze zm.

7 Dz. U. z 2022 r. poz. 623.

1. WPROWADZENIE

Pytanie definiujące cel główny kontroli

Czy prawidłowo, rzetelnie i skutecznie realizowano zadania związane z zapewnieniem bezpieczeństwa informacji oraz ciągłości działania systemów informatycznych w jednostkach samorządu terytorialnego?

Pytania definiujące cele szczegółowe kontroli

1. Czy podjęto prawidłowe, rzetelne i skuteczne działania dla zapewnienia organizacji bezpieczeństwa informacji oraz dla zapewnienia ciągłości działania systemów informatycznych, tj. czy przeprowadzono odpowiednie analizy oraz czy opracowano i przyjęto do stosowania odpowiednie procedury, polityki, instrukcje oraz określono i zapewniono niezbędne zasoby osobowe i techniczne?
2. Czy prawidłowo, rzetelnie i skutecznie wdrożono przyjęte rozwiązania organizacyjne i techniczne, tj. czy są one faktycznie stosowane i egzekwowane?
3. Czy są cyklicznie podejmowane prawidłowe działania mające na celu zapobieganie incydentom bezpieczeństwa informacji (szkolenia, analiza incydentów, audyty, analiza ryzyka)?

Jednostki kontrolowane

Kontrolą objęto 24 jednostki: 17 urzędów gmin i 7 starostw powiatowych.

Okres objęty kontrolą

Od 1 stycznia 2023 r. do dnia zakończenia kontroli[8].

Działanie państwa w dużej i coraz większej mierze opiera się o wykorzystanie i przetwarzanie informacji zgromadzonych w rejestrach publicznych i innych zbiorach danych, do których dostęp następuje poprzez systemy informatyczne. Stale rośnie zapotrzebowanie na wysoką dostępność danych i systemów informatycznych, bez których nie jest możliwa obsługa obywateli i załatwianie większości spraw. Stale rośnie też liczba zagrożeń dla bezpieczeństwa informacji. Coraz większym wyzwaniem staje się zapewnienie bezpieczeństwa informacji oraz zapewnienie ciągłości działania pracy urzędów. Stosowane metody zabezpieczeń powinny umożliwić zachowanie integralności, poufności i dostępności danych.

Zarządzanie ciągłością działania systemów informatycznych obejmuje analizę zagrożeń (tj. potencjalnych ryzyk mających wpływ na prowadzenie normalnej działalności) i ich wpływu na działalność urzędu, jak też opiera się na zdefiniowaniu i wdrożeniu niezbędnych zabezpieczeń zarówno prewencyjnych, jak i na zapewnieniu reagowania adekwatnie do ujawnionych potencjalnych zagrożeń. Brak zapewnienia ciągłości działania oraz komunikacji w sytuacji kryzysowej może doprowadzić do przerwy lub do całkowitego zaprzestania działalności, stąd też należy opracować i wdrożyć odpowiednie strategie i procedury działania.

Zidentyfikowane przez NIK zagrożenia dla prawidłowego funkcjonowania urzędów dotyczą m.in. tego, że kierownicy nie nadają należytej wagi bezpieczeństwu informacji ani zapewnieniu ciągłości działania, nie wdrażają i nie aktualizują polityk i procedur, nie zapewniają odpowiednich narzędzi IT lub nie w pełni je stosują. Skutkiem tych zaniechań może być utrata danych, a także istotne utrudnienia w obsłudze obywateli i pracy urzędów. Ataki hakerskie, katastrofy (zalanie, pożar, itp.), zagrożenia epidemiologiczne oraz wyciek lub utrata danych, w tym danych osobowych, mogą skutecznie zakłócić realizację zadań j.s.t. Przygotowanie planu ciągłości działania jest niezbędne dla zapewnienia działania urzędu w sytuacji kryzysowej, np. w wypadku zaistnienia zagrożeń hybrydowych.

Jednostka, aby zabezpieczyć swoje informacje powinna zastosować podejście systemowe, w ramach którego będzie zarządzać kompleksowo posiadanymi aktywami informacyjnymi, infrastrukturą przeznaczoną do ich przetwarzania oraz ryzykiem dotyczącym bezpieczeństwa informacji. Oprócz informacji, których wymóg ochrony zapisany jest wprost w przepisach, istnieją także inne informacje, równie ważne, o których ochronę każdy urząd powinien zadbać samodzielnie. Praktyka ograniczania zakresu ochrony jedynie do niektórych informacji (np. tylko danych osobowych) może mieć poważne konsekwencje dla właściwego szacowania ryzyka, dzielenia zasobów i zapewnienia ciągłości działania urzędów.

Wyniki poprzednich kontroli[9] NIK wykazały m.in., że dane gromadzone i przetwarzane w bazach i systemach komputerowych urzędów gmin i miast, a także w starostwach były słabo chronione. Wskazano na wieloletnie zaniedbania związane z ochroną danych, nieświadomość zagrożeń i brak jednoznacznych wytycznych – wybrane elementy systemu ochrony danych w jednostkach samorządowych były złym stanie. Brakowało skutecznego systemu zarządzania incydentami bezpieczeństwa informacji (identyfikacji i reagowania na ataki).

[8] 20 września 2024 r.

[9] Nr P/18/006/KAP *Zarządzanie bezpieczeństwem informacji w jednostkach samorządu terytorialnego*; nr I/23/002/LBI *Zapewnienie ochrony i prawidłowego przetwarzania danych, w tym danych osobowych gromadzonych w formie elektronicznej przez jednostki samorządu terytorialnego oraz podległe jednostki organizacyjne na stronach internetowych, poczcie elektronicznej oraz w związku z odbywającymi się sesjami organów uchwałodawczych*; nr I/23/001/LSZ *Zapewnienie bezpieczeństwa teleinformatycznego przez jednostki samorządu terytorialnego województwa zachodniopomorskiego*.

2. OCENA OGÓLNA

Niewystarczająca realizacja zadań jst w zakresie zapewnienia bezpieczeństwa informacji i ciągłości działania

Zadania w zakresie zapewnienia bezpieczeństwa informacji nie były skutecznie, rzetelnie i prawidłowo wykonywane w większości skontrolowanych urzędów jednostek samorządu terytorialnego, a NIK negatywnie oceniła przygotowanie do zapewnienia ciągłości działania systemów informatycznych w 71 % tych urzędów. Istotne nieprawidłowości ujawniono w 23 z 24 objętych kontrolą jednostek, w tym w przypadku dwóch urzędów sformułowano negatywną ocenę ogólną[10].

Działania w zakresie organizacji zapewnienia bezpieczeństwa informacji nie były w pełni skutecznie, należycie i prawidłowo realizowane. W połowie skontrolowanych urzędów jst nie podjęto odpowiednich analiz i nie zidentyfikowano części posiadanych zbiorów danych i ich wagi pod kątem zapewnienia odpowiedniej ochrony, co NIK oceniła jako działanie nierzetelne. W 33 % urzędów nie opracowano lub nie wdrożono Systemu Zarządzania Bezpieczeństwa Informacji, a w prawie 20 % urzędów nie był on poddawany przeglądowi i aktualizacji, co było niezgodne odpowiednio z § 19 ust. 1 oraz § 19 ust. 2 pkt 1 obowiązującego rozporządzenia KRI. W 71 % kontrolowanych urzędów brak było ustanowionych polityk ciągłości działania, a w połowie jednostek nie opracowano planów zapewnienia ciągłości oraz planów odtworzeniowych, co NIK oceniła jako działanie nierzetelne. Nawet jeżeli plany odtworzeniowe opracowano, to w większości nie były one testowane. Tym samym brak było potwierdzenia, że w przypadku awarii lub sytuacji kryzysowej będzie możliwe szybkie i skuteczne przywrócenie działania systemów informatycznych.

Przyjęte rozwiązania dotyczące bezpieczeństwa informacji oraz ciągłości działania nie były w pełni prawidłowo wdrożone i należycie stosowane, pomimo że w 92 % urzędów wyznaczono pracowników odpowiedzialnych za bezpieczeństwo informacji i ciągłość działania. W 20 podmiotach (tj. 83 %) wystąpiły nieprawidłowości w zakresie: zabezpieczenia serwerowni, sporządzania kopii zapasowych, braku w umowach na zakup usług IT lub serwis sprzętu/oprogramowania odpowiednich zapisów w zakresie bezpieczeństwa informacji, co stanowiło naruszenie wymogów obowiązującego rozporządzenia KRI. W dziewięciu urzędach nie w pełni przestrzegano ustalonych zasad dostępu do systemów informatycznych. W dziewięciu jednostkach nie zidentyfikowano kluczowych elementów infrastruktury i usług IT, co NIK oceniła jako nierzetelne. Tylko w trzech urzędach monitorowano oprogramowanie na służbowych telefonach komórkowych i tabletach. Pozytywnie należy ocenić, że w 20 urzędach (83 %) użytkownicy nie mieli możliwości instalacji dowolnego oprogramowania, co było zgodne z § 19 ust. 2 pkt 4 obowiązującego rozporządzenia KRI, a w 21 podmiotach (87 %), zgodnie z § 19 ust. 2 pkt 8 obowiązującego rozporządzenia KRI, określono szczegółowe zasady i procedury korzystania przez pracowników z urządzeń przenośnych poza siedzibą urzędu.

[10] Stwierdzono łącznie 222 nieprawidłowości.

W kontrolowanych urzędach podejmowano cykliczne działania w celu zapobiegania incydentom bezpieczeństwa informacji, jednak w 16 urzędach stwierdzono nieprawidłowości. W 71 % kontrolowanych urzędów prowadzono okresowe analizy ryzyka utraty integralności, poufności, dostępności informacji oraz wdrożono procedury zgłaszania naruszenia bezpieczeństwa informacji. W 37 % urzędów wystąpiły nieprawidłowości w zakresie okresowego audytu bezpieczeństwa informacji. W 42 % urzędów nie zapewniono pracownikom szkoleń dotyczących bezpieczeństwa informacji, co było niezgodne z § 19 ust. 2 pkt 6 tego rozporządzenia.

3. SYNTEZA

Rozwiązania organizacyjne i techniczne w zakresie zapewnienia bezpieczeństwa przetwarzania informacji oraz zapewnienia ciągłości

Niezidentyfikowanie wszystkich zbiorów danych, które powinny podlegać zabezpieczeniu w połowie urzędów

W 12 objętych kontrolą urzędach (50 %), nie dokonano pełnej identyfikacji aktywów informacyjnych wymagających ochrony lub zidentyfikowanym zbiorom danych nie przypisano odpowiedniego poziomu ochrony, co było nierzetelne. Pomijano przy tym inne dane niż osobowe informacje wymagające ochrony. [str. 14–15]

Brak ustanowienia i przeglądu SZBI w 33 % urzędów

W okresie objętym kontrolą w ośmiu jednostkach nie opracowano i nie wdrożono Systemu Zarządzania Bezpieczeństwem Informacji, a w trzech jednostkach, gdzie SZBI został ustanowiony, nie dokonano jego przeglądu pod względem adekwatności i skuteczności, co było niezgodne z § 19 ust. 1 obowiązującego rozporządzenia KRI. [str. 15–18]

Prawidłowo wyznaczono IOD i osoby odpowiedzialne za kontakt z podmiotami krajowego systemu cyberbezpieczeństwa

We wszystkich 24 kontrolowanych urzędach zgodnie z przepisami wyznaczono osobę na stanowisko IOD. Osoby wyznaczone na IOD podlegały najwyższemu kierownictwu tych jednostek, tym samym umożliwiono im wykonywanie obowiązków w sposób niezależny. We wszystkich 24 urzędach zostały wyznaczone także osoby odpowiedzialne za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa w zakresie związanym z realizacją przez urzędy zadań publicznych zależnych od systemu informacyjnego i systemu teleinformacyjnego wraz z przetwarzanymi w nim danymi w postaci elektronicznej. [str. 18–19]

Brak ustanowienia polityk ciągłości działania (71 % urzędów), planów zapewnienia ciągłości oraz planów odtworzeniowych (50 % urzędów)

W 71 % kontrolowanych urzędów brak było ustanowionych polityk ciągłości działania a w połowie nie opracowano planów zapewnienia ciągłości oraz planów odtworzeniowych, co było nierzetelne. Nawet w sytuacji, gdy plany takie były ustanowione (50 % urzędów) nie podlegały one testowaniu, tym samym brak było potwierdzenia, że w przypadku wystąpienia awarii pozwolą na szybkie i skuteczne przywrócenie działania systemów informatycznych. [str. 21–23]

Wdrożenie przyjętych rozwiązań organizacyjnych i technicznych w zakresie bezpieczeństwa informacji

Nieprawidłowości w zakresie zarządzania uprawnieniami użytkowników

W trakcie kontroli ustalono, że spośród 235 objętych badaniem pracowników wykonujących zadania w systemach informatycznych 11 z nich, tj. 5 %, miało możliwość zainstalowania na użytkowanych komputerach dowolnego oprogramowania, co było niezgodne z wymaganiami określonymi w § 19 ust. 2 pkt 4 obowiązującego rozporządzenia KRI. W wyniku badania przyznanych uprawnień dostępu do korzystania z systemów informatycznych, dokonanego na łącznej próbie 359 pracowników kontrolowanych urzędów, stwierdzono że w przypadku ośmiu osób nadane uprawnienia były nieadekwatne do zadań określonych w zakresach czynności tych osób. W przypadku 240 osób, które zakończyły zatrudnienie w kontrolowanych urzędach, stwierdzono, iż 52 byłym pracownikom (tj. 22 %) w 15 urzędach konta nie zostały zablokowane i pozostawały wciąż aktywne. [str. 23–25]

Niepełne przestrzeganie wymogów w zakresie haseł dostępu w 37 % urzędów

Pomimo ustanowienia wymogów w zakresie uzyskiwania dostępu do systemów informatycznych, w dziewięciu kontrolowanych urzędach, (37 %) zasady te nie były w pełni przestrzegane. Nieprawidłowości w tym zakresie dotyczyły przede wszystkim stosowania przez użytkowników haseł do systemów informatycznych krótszych niż wymagane. [str. 25–26]

Serwerownie nie były właściwie zabezpieczone w połowie urzędów

W połowie kontrolowanych urzędów zastosowano zabezpieczenia fizyczne serwerowni, które w niewystarczającym stopniu chroniły te pomieszczenia, co było niezgodne z § 19 ust. 2 pkt 9 obowiązującego rozporządzenia KRI. [str. 27–28]

Brak zapisów gwarantujących poufność informacji w umowach z podmiotami zewnętrznymi w przypadku 30 % umów

W 11 urzędach (46 %) w umowach na zakup usług informatycznych, zakup lub serwis sprzętu komputerowego/oprogramowania stwierdzono brak zapisów gwarantujących zabezpieczenie poufności informacji uzyskanych przez wykonawców w związku z realizacją tych umów, co było niezgodne z § 19 ust. 2 pkt 10 obowiązującego rozporządzenia KRI. Zapisów takich nie zawarto łącznie w 30 umowach spośród 101 objętych badaniem (tj. 30 %). [str. 28]

Nieprawidłowości w zakresie tworzenia, przechowywania lub testowania kopii zapasowych

W 12 urzędach (50 %) stwierdzono nieprawidłowości polegające na niespełnieniu wymogów wynikających z § 19 ust. 2 pkt 12 lit. b obowiązującego rozporządzenia KRI, które polegały na:

- niewłaściwym przechowywaniu kopii zapasowych danych z systemów informatycznych, tj. w sposób, który nie minimalizuje ryzyka utraty informacji i stwarza zagrożenie, że w przypadku zdarzeń losowych, np. pożaru lub zalania, urząd może utracić zarówno dane źródłowe, jak i ich kopie zapasowe. W siedmiu urzędach (29 %) stwierdzono, że sporządzane kopie zapasowe przechowywane były w serwerowniach, a więc w miejscach wytwarzania danych lub w innym miejscu do którego dostęp miały osoby nieupoważnione. Kopie zapasowe powinny być przechowywane w innej lokalizacji, w odległości pozwalającej uniknąć uszkodzeń spowodowanych katastrofą, która dotknęła ośrodek podstawowy;
- niesporządzaniu kopii zapasowych lub tworzeniu ich niezgodnie z przyjętymi procedurami – w trzech urzędach;
- braku testowania kopii zapasowych w sześciu urzędach. [str. 29]

Nie zidentyfikowano kluczowych elementów infrastruktury i usług IT w 37 % urzędów

W ramach zapewnienia ciągłości działania, w dziewięciu kontrolowanych urzędach (37 %) nie zidentyfikowano w sposób udokumentowany kluczowych elementów infrastruktury i usług IT oraz nie ustalono ich zabezpieczenia pod kątem wpływu czynników zewnętrznych, co było nierzetelne. [str. 30]

Nie monitorowano służbowych telefonów komórkowych/tabletów

Jedynie w trzech urzędach wprowadzono rozwiązania techniczne umożliwiające monitorowanie oprogramowania wykorzystywanego na telefonach służbowych/tabletach. [str. 27]

W 88 % urzędów ustanowiono zasady pracy na odległość i zabezpieczenie danych na urządzeniach mobilnych

W 19 urzędach (88 %) zgodnie z § 19 ust. 2 pkt 8 obowiązującego rozporządzenia KRI określono szczegółowe zasady i procedury korzystania przez pracowników z urządzeń przenośnych (dot. m.in. komputerów przenośnych) poza jego siedzibą, gwarantujących bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość, a także stosowano rozwiązania polegające na szyfrowaniu dysków twardych komputerów przenośnych. [str. 26–27]

Podejmowanie działań mających na celu zapobieganie incydentom bezpieczeństwa informacji

W 71 % urzędów prowadzono okresowe analizy ryzyka utraty integralności, poufności lub dostępności informacji

W 17 urzędach (71 %) prowadzono okresowe analizy ryzyka utraty integralności, poufności lub dostępności informacji zgodnie z § 19 ust. 2 pkt 3 obowiązującego rozporządzenia KRI. Przeprowadzenie analizy umożliwiło ustalenie istotnych ryzyk mających wpływ na zapewnienie bezpieczeństwa informacji. Dokonano oceny istotności ryzyk oraz podjęto działania w celu zminimalizowania ich wpływu na działalność urzędu. [str. 31–32]

Niewystarczająca liczba szkoleń z bezpieczeństwa informacji w 37 % urzędów

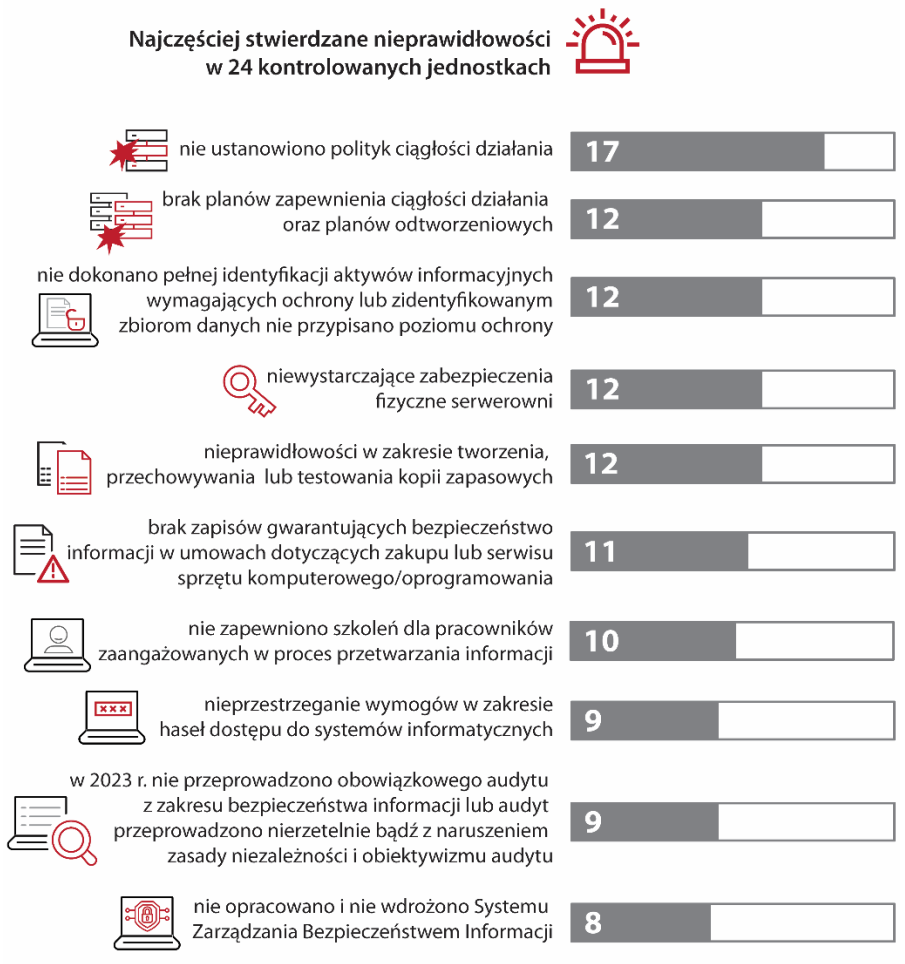
W 10 urzędach (42 %) nie zapewniono szkoleń dla pracowników zaangażowanych w proces przetwarzania informacji, co było niezgodne z § 19 ust. 2 pkt 6 obowiązującego rozporządzenia KRI. [str. 33–34]

Nieprawidłowości w zakresie audytów bezpieczeństwa informacji w 37 % urzędów

W dziewięciu urzędach (37 %) w 2023 r. nie przeprowadzono corocznego obowiązkowego audytu z zakresu bezpieczeństwa informacji, co było niezgodne z § 19 ust. 2 pkt 14 obowiązującego rozporządzenia KRI lub audyt prowadzono nierzetelnie, bądź z naruszeniem zasady niezależności i obiektywizmu audytu. [str. 35]

Na infografice nr 1 przedstawiono liczbę urzędów, w których wystąpiły najczęściej stwierdzane nieprawidłowości.

Infografika nr 1



Źródło: opracowanie własne NIK na podstawie wyników kontroli.

4. WNIOSKI

Po kontroli NIK wnioskuje o:

Minister Cyfryzacji

Biorąc pod uwagę skalę i zakres zidentyfikowanych nieprawidłowości, zasadne jest stałe wspieranie urzędów j.s.t przez Ministra Cyfryzacji w zakresie wdrażania rozwiązań organizacyjnych i technicznych dotyczących bezpieczeństwa informacji oraz zapewnienia ciągłości działania urzędów jst.

Starostowie, prezydenci miast, burmistrzowie i wójtowie

1) opracowanie i wdrożenie Systemu Zarządzania Bezpieczeństwem Informacji, zgodnie z § 19 ust. 1 w związku z ust. 3 obowiązującego rozporządzenia KRI;
2) zapewnienie dokonywania okresowego przeglądu i aktualizacji Systemu Zarządzania Bezpieczeństwem Informacji zgodnie z § 19 ust. 2 pkt 1 obowiązującego rozporządzenia KRI;
3) ustanowienie polityk ciągłości działania oraz opracowanie i wdrożenie planów zapewnienia ciągłości działania urzędów, planów odtworzeniowych oraz zapewnienie ich okresowego testowania;
4) zapewnienie pracownikom zaangażowanym w proces przetwarzania informacji odpowiednich szkoleń w tym zakresie, zgodnie z § 19 ust. 2 pkt 6 obowiązującego rozporządzenia KRI;
5) prowadzenie okresowych analiz ryzyka utraty integralności, poufności lub dostępności informacji, zgodnie z § 19 ust. 2 pkt 3 obowiązującego rozporządzenia KRI;
6) wdrożenie rozwiązań zapewniających odpowiednie zabezpieczenie pomieszczeń serwerowni, zgodnie z § 19 ust. 2 pkt 9 obowiązującego rozporządzenia KRI;
7) regularne testowanie kopii zapasowych oraz przechowywanie ich poza miejscem wytworzenia;
8) zapewnienie prowadzenia przynajmniej raz w roku okresowego audytu wewnętrznego z zakresu bezpieczeństwa informacji, zgodnie z § 19 ust. 2 pkt 14 obowiązującego rozporządzenia KRI;
9) przyznawanie i odbieranie pracownikom urzędów uprawnień w systemach informatycznych adekwatnie do realizowanych zadań, zgodnie z § 19 ust. 2 pkt 4 obowiązującego rozporządzenia KRI;
10) egzekwowanie wdrożonych rozwiązań organizacyjnych i technicznych w zakresie bezpieczeństwa informacji;
11) zawieranie w umowach o świadczenie usług informatycznych postanowień gwarantujących odpowiedni poziom bezpieczeństwa informacji, zgodnie z § 19 ust. 2 pkt 10 obowiązującego rozporządzenia KRI;
12) objęcie nadzorem oprogramowania instalowanego na urządzeniach mobilnych (komórkowe telefony służbowe/tablety).

5. WAŻNIEJSZE WYNIKI KONTROLI

5.1. ROZWIĄZANIA ORGANIZACYJNE I TECHNICZNE W ZAKRESIE ZAPEWNIENIA BEZPIECZEŃSTWA PRZETWARZANIA INFORMACJI ORAZ ZAPEWNIENIA CIĄGŁOŚCI DZIAŁANIA W URZĘDACH GMIN/STAROSTWACH POWIATOWYCH I ICH STOSOWANIE

W większości urzędów stwierdzono nieprawidłowości w zakresie zapewnienia bezpieczeństwa informacji oraz zapewnienia ciągłości działania systemów informatycznych

W 92 % kontrolowanych urzędów stwierdzono nieprawidłowości w zakresie organizacji zapewnienia bezpieczeństwa przetwarzania informacji oraz zapewnienia ciągłości działania ich systemów informatycznych. W pięciu urzędach NIK sformułowała w tym obszarze ocenę negatywną. W ponad połowie urzędów (13 urzędów, tj. 54 %) nie opracowano i nie wdrożono Systemu Zapewnienia Bezpieczeństwa Informacji lub nie był on aktualizowany, bądź dokonany przegląd SZBI był nierzetelny. W połowie urzędów nie zidentyfikowano zbiorów danych, które podlegają ochronie. Pozytywnie należy ocenić, że we wszystkich badanych urzędach wyznaczono osoby odpowiedzialne za bezpieczeństwo informacji i ciągłość działania, IOD oraz osoby odpowiedzialne za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa. W większości urzędów (17 urzędów, tj. 71 %) brak było ustanowionych polityk ciągłości działania, a w połowie nie opracowano planów zapewnienia ciągłości oraz planów odtworzeniowych. W 58 % urzędów, w których plany takie ustanowiono, nie były one jednak testowane.

Identyfikowanie zbiorów danych podlegających zabezpieczeniu

Identyfikacja zbiorów danych przetwarzanych w jednostce jest kluczowa dla zapewnienia bezpieczeństwa informacji. Działanie takie pozwala na określenie istotności danych oraz wprowadzenia odpowiednich mechanizmów pozwalających na ich ochronę. Zidentyfikowanym zbiorom danych należy przypisać odpowiedni poziom ochrony, zgodny z ich istotnością. Jak wskazano w pkt A.8.1.1 i A.8.2.1 załącznika A normy[11] PN-EN ISO/IEC 27001:2017 należy zidentyfikować informacje, aktywa związane z informacjami i środkami przetwarzania informacji oraz sporządzić i utrzymywać ewidencję tych aktywów. Informacje takie klasyfikuje się z uwzględnieniem wymagań prawnych, wartości, krytyczności i wrażliwości na nieuprawnione ujawnienie lub modyfikację.
W 12 objętych kontrolą urzędach[12] (50 %) nie dokonano pełnej identyfikacji aktywów informacyjnych wymagających ochrony lub zidentyfikowanym zbiorom danych nie przypisano odpowiedniego poziomu ochrony, co było nierzetelne. Pomijano na ogół informacje wymagające ochrony – inne niż dane osobowe, takie jak powierzone przez kontrahentów tajemnice przedsiębiorstwa, zasady bezpieczeństwa fizycznego i informatycznego w jednostce, informacje finansowe z deklaracji podatkowych itp.

[11] Polska Norma PN-EN ISO/IEC 27001:2017 *Technika Informatyczna. Techniki bezpieczeństwa. Systemy zarządzania bezpieczeństwem informacji. Wymagania.*

[12] Dotyczy to starostw w: Kłodzku, Ostrołęce i Sępólnie Krajeńskim oraz UM/UG: Czechowice-Dziedzice, Józefów, Otwock, Nowa Ruda, Osie, Sośnicowice, Świecie, Świętochłowice, Szydłowiec.

Przykład

W **Starostwie Powiatowym w Ostrołęce** nie zidentyfikowano i nie sklasyfikowano z uwzględnieniem wymagań określonych w normie PN-EN ISO/EIC 27001:2017 wszystkich zbiorów danych, co było nierzetelne. Wicestarosta wyjaśnił, że w urzędzie nie posiadano zatwierdzonej przez starostę klasyfikacji wszystkich posiadanych i przetwarzanych zbiorów danych. Jako przyczynę wskazał braki kadrowe w zakresie informatyki i brak środków finansowych na zadania związane z zapewnieniem bezpieczeństwa informacji. Dodał także, że (...) *zadania są zaplanowane do realizacji dzięki pozyskanym przez Powiat Ostrołęcki środkom z programu „Cyberbezpieczny Samorząd".*

W pozostałych 12 kontrolowanych urzędach identyfikowano zbiory danych podlegających zabezpieczeniu.

Przykład

W **Urzędzie Miejskim w Głogowie** identyfikacja zbiorów danych wymagających ochrony w Urzędzie dokonywana była corocznie jako element zarządzania ryzykiem w bezpieczeństwie informacji. Oceny wagi tych zbiorów oraz systemów teleinformatycznych, w których były one przetwarzane, dokonywano pod kątem wpływu braku funkcjonowania lub nieprawidłowego ich funkcjonowania na: bezpieczeństwo ludzi oraz zasobów informacyjnych; ciągłości działania oraz realizowania funkcji i zadań Urzędu, które byłyby niemożliwe do realizacji bez systemu teleinformatycznego; możliwości realizowania konstytucyjnych praw i obowiązków obywatela oraz zaufania obywateli do władzy publicznej.

W wyniku przeprowadzonej w wyżej opisany sposób inwentaryzacji, zidentyfikowano 55 zbiorów danych i systemów informatycznych o kategorii krytycznej wymagających ochrony.

Dodatkowo w ramach Rejestru Czynności Przetwarzania Danych Osobowych zidentyfikowano 283 czynności, w których przetwarzano dane osobowe. Dla każdej czynności wskazano m.in.: cel przetwarzania, podstawę prawną przetwarzania, właściciela procesu, kategorie osób, danych i odbiorców, sposób przetwarzania i pozyskiwania danych, okres ich przechowywania, ogólny opis środków bezpieczeństwa danych oraz informacje na temat ewentualnego transferu danych do krajów trzecich.

Systemy Zarządzania Bezpieczeństwem Informacji w urzędach

Jednostka, aby zabezpieczyć swoje informacje powinna zastosować podejście systemowe, w ramach którego będzie zarządzać kompleksowo posiadanymi aktywami informacyjnymi, infrastrukturą przeznaczoną do ich przetwarzania oraz ryzykiem dotyczącym bezpieczeństwa informacji. System Zarządzania Bezpieczeństwem Informacji określa wymagania oraz zasady inicjowania, wdrażania, utrzymania i poprawy zarządzania bezpieczeństwem informacji w jednostce, oraz zawiera najlepsze praktyki celów stosowania zabezpieczeń.

W ośmiu objętych kontrolą urzędach[13] (33 %) nie opracowano i nie wdrożono Systemu Zarządzania Bezpieczeństwem Informacji, o którym mowa w § 20 ust. 1 w zw. z ust. 3 wcześniejszego rozporządzenia KRI

[13] Dotyczy to starostw w: Kłodzku, Ostrołęce, Sępólnie Krajeńskim, Sochaczewie oraz UM/UG: Nowa Ruda, Otwock, Sośnicowice, Świętochłowice.

oraz § 19 ust. 1 w związku z ust. 3 obowiązującego rozporządzenia KRI, w szczególności nie ustanowiono polityki bezpieczeństwa informacji. W myśl tych przepisów 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. Ponadto, § 20 ust. 3 wcześniejszego rozporządzenia KRI oraz § 19 ust. 3 obwiązującego rozporządzenia KRI wskazuje, że wymagania określone w ww. ust. 1 uznaje się za spełnione, jeżeli system zarządzania bezpieczeństwem informacji został opracowany na podstawie Polskiej Normy PN-EN ISO/IEC 27001, a ustanawianie zabezpieczeń, zarządzanie ryzykiem oraz audytowanie odbywa się na podstawie Polskich Norm związanych z tą normą[14].

Opracowane i wdrożone w tych ośmiu jednostkach regulacje nie obejmowały wszystkich informacji jakie są przetwarzane w urzędzie[15], lecz dotyczyły głównie danych osobowych.

Kontrolowani wskazywali m.in., że planowane są, bądź zostały podjęte prace dla przygotowania SZBI, w tym polityki bezpieczeństwa informacji.

Przykłady

Starosta sępoleński poinformował m.in., że powiat sępoleński zawarł umowę na powierzenie grantu na Rozwój Cyfrowy 2021–2027 (FERC) Priorytet II: Zaawansowane usługi cyfrowe Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa konkurs grantowy w ramach Projektu grantowego „Cyberbezpieczny Samorząd". Celem projektu grantowego jest zwiększenie poziomu bezpieczeństwa informacji jst poprzez wzmocnienie odporności oraz zdolności do skutecznego zapobiegania i reagowania na incydenty w systemach informacyjnych.

W ramach ww. zadania zaplanowano m.in.:

- opracowanie, wdrożenie, przegląd, aktualizację dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji;
- przeprowadzenie niezależnych audytów zgodności z wymogami KRI;
- przeprowadzenie audytu SZBI;
- przeprowadzenie szkoleń specjalistycznych pracowników działu IT;
- przeprowadzenie szkoleń z zakresu cyberbezpieczeństwa dla kadry kierowniczej i pracowników starostwa powiatowego;
- organizację kampanii phishingowych dla pracowników starostwa powiatowego.

Starosta ostrołęcki poinformował m.in., że opracowanie, ustanowienie i wdrożenie Systemu Zarządzania Bezpieczeństwem Informacji nastąpi przez Wydział Informatyki i Cyberbezpieczeństwa w ramach realizacji programu „Cyberbezpieczny Samorząd". Program realizowany będzie do końca czerwca 2026 r.

[14] 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.

[15] M.in. dotyczących konfiguracji infrastruktury informatycznej w tym serwerów, zarządzania hasłami dostępu do systemów IT, treści umów z dostawcami, warunków zastrzeżonych przez dostawców, tajemnic wynikających z innych aktów prawnych, jak np. prawa własności intelektualnej, zasad bezpieczeństwa fizycznego w obiekcie, korespondencji służbowej czy stosowanych zabezpieczeń systemów informatycznych.

W pozostałych 16 urzędach opracowano i wdrożono System Zarządzania Bezpieczeństwem Informacji (SZBI).

Na infografice nr 2 przedstawiono cykl funkcjonowania SZBI.

Infografika nr 2

Źródło: opracowanie własne NIK.

Aktualizacja regulacji wewnętrznych stanowiących System Zarządzania Bezpieczeństwem Informacji

Zgodnie z § 20 ust. 2 pkt 1 wcześniejszego rozporządzenia KRI oraz § 19 ust. 2 pkt 1 obowiązującego rozporządzenia KRI, podmiot zobowiązany jest do zapewnienia aktualizacji regulacji wewnętrznych w zakresie dotyczącym zmieniającego się otoczenia. Badania kontrolne w tym zakresie obejmują podjęte przez urząd działania związane z aktualizacją regulacji wewnętrznych w zakresie zmieniającego się otoczenia będące konsekwencją wyników szacowania ryzyka, wniosków z przeglądów SZBI, zaleceń poaudytowych, wniosków z analizy incydentów naruszenia bezpieczeństwa informacji.

Stosownie do załącznika A PN-ISO/IEC 27001:2017, punkt A.5.1.2, polityki bezpieczeństwa informacji należy poddawać przeglądom w zaplanowanych odstępach czasu lub wtedy, gdy wystąpią istotne zmiany, aby zapewnić, że nadal są właściwe, adekwatne i skuteczne.

W okresie objętym kontrolą spośród 16 kontrolowanych jednostek[16], w których opracowano i wdrożono System Zarządzania Bezpieczeństwem Informacji, w trzech[17] jednostkach nie dokonano jego przeglądu pod względem adekwatności i skuteczności. Ponadto, w dwóch urzędach, w których dokonano przeglądu SZBI, był on nierzetelny[18].

[16] Dotyczy to starostw w: Lubinie, Wąbrzeźnie, Wodzisławiu Śląskim oraz UM/UG: Czechowice-Dziedzice, Głogów, Józefów, Kamienna Góra, Kcynia, Koronowo, Oława, Osie, Pyskowice, Szydłowiec, Świecie, Zbrosławice, Żyrardów.

[17] Dotyczy to starostwa w Wąbrzeźnie oraz UM/UG: Oława i Osie.

[18] Dotyczy Starostwa Powiatowego w Lubinie oraz Urzędu Miasta Kamienna Góra.

Wewnętrzne uregulowania dotyczące ochrony danych osobowych

We wszystkich 24 kontrolowanych jednostkach wprowadzono regulacje w zakresie ochrony danych osobowych. Uregulowania te wprowadzono np. w takich dokumentach jak: Polityka Bezpieczeństwa Danych Osobowych, Regulamin Ochrony Danych Osobowych, Polityka Ochrony Danych Osobowych, Instrukcja Zarządzania Systemami IT.

Przykład

W **Urzędzie Miejskim w Oławie** sporządzono dokumentację w zakresie ochrony danych osobowych uwzględniającą wymogi RODO. Była ona częścią SZBI. Jeden z głównych elementów tej dokumentacji, tj. Polityka Ochrony Danych Osobowych zawierała m.in. wykaz budynków i pomieszczeń, w których są przetwarzane dane osobowe, strukturę zbiorów danych osobowych, sposób przepływu danych osobowych pomiędzy systemami, środki techniczne i organizacyjne niezbędne dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych. Ponadto wprowadzono procedury nadawania i odbierania upoważnień do przetwarzania danych osobowych, procedury postępowania w sytuacji naruszenia ochrony danych osobowych, procedury zawierania i prowadzenia rejestru umów powierzenia przetwarzania danych osobowych i inne. Dokumentacja ta została zatwierdzona przez burmistrza i zakomunikowana odpowiedzialnym pracownikom urzędu.

Wyznaczenie Inspektora Ochrony Danych

Zgodnie z art. 37 ust. 1 i 5 RODO oraz art. 8 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych[19] we wszystkich 24 kontrolowanych urzędach wyznaczono osobę na stanowisko IOD[20]. Funkcję IOD pełnili pracownicy kontrolowanych urzędów lub zadania te powierzano firmom zewnętrznym, na podstawie zawieranych umów. Osoby pełniące funkcję IOD posiadały odpowiednie kwalifikacje, potwierdzone szkoleniami oraz praktyką zawodową.

W zakresach obowiązków osób pełniących funkcję IOD ustalono m.in. monitorowanie przestrzegania przepisów o ochronie danych osobowych; informowanie administratora, podmiotów przetwarzających oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach wynikających z przepisów o ochronie danych osobowych, doradzanie im

[19] Dz. U. z 2019 r. poz. 1781.

[20] Do zadań Inspektora Ochrony Danych (IOD) należy:

a) informowanie administratora, podmiotu przetwarzającego oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy niniejszego rozporządzenia oraz innych przepisów Unii lub państw członkowskich o ochronie danych i doradzanie im w tej sprawie;
b) monitorowanie przestrzegania niniejszego rozporządzenia, innych przepisów Unii lub państw członkowskich o ochronie danych oraz polityk administratora lub podmiotu przetwarzającego w dziedzinie ochrony danych osobowych, w tym podział obowiązków, działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty;
c) udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania zgodnie z art. 35 RODO;
d) współpraca z organem nadzorczym;
e) pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, o których mowa w art. 36 RODO, oraz w stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach.

Artykuł 38 ust. 3 RODO stanowi, że inspektor ochrony danych bezpośrednio podlega najwyższemu kierownictwu. Ta bezpośrednia podległość zapewnia najwyższemu kierownictwu, będącemu jednocześnie administratorem (prezydentowi, burmistrzowi, wójtowi, staroście) wiedzę na temat porad i zaleceń IOD.

w tej sprawie i rekomendowanie określonych działań; opracowywanie polityk i procedur z zakresu ochrony danych osobowych; zbieranie informacji w celu identyfikacji procesów przetwarzania; podnoszenie świadomości osób przetwarzających dane osobowe; współpraca z organem nadzorczym oraz pełnienie funkcji punktu kontaktowego pomiędzy administratorem a Urzędem Ochrony Danych Osobowych.

Zgodnie z art. 38 ust. 6 RODO, osoba wyznaczona na IOD może wykonywać inne zadania i obowiązki, jednak administrator danych (tj. kierownik jednostki) musi zapewnić, by takie zadania i obowiązki nie powodowały konfliktu interesów.

We wszystkich kontrolowanych jednostkach osoby wyznaczone na IOD podlegały najwyższemu kierownictwu tych jednostek, tym samym umożliwiono im wykonywanie obowiązków w sposób niezależny.

W ośmiu[21] z 24 urzędów (33 %) nastąpił konflikt interesów lub naruszono zasadę niezależności i obiektywności audytu określoną w *Standardach audytu wewnętrznego dla jednostek finansów publicznych*[22] oraz w pkt 9.2 lit. e normy ISO/IEC 27001, gdyż IOD m.in. uczestniczyli w prowadzeniu audytów z zakresu bezpieczeństwa informacji. Prowadzenie przez IOD audytu wewnętrznego z zakresu bezpieczeństwa nie powinno mieć miejsca, o ile IOD oceniał realizowane przez siebie wcześniej zadania. Działanie takie stanowi bowiem konflikt interesów i może naruszać zasadę bezstronności.

Wyznaczenie osób odpowiedzialnych za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa

Zgodnie z art. 21 ustawy o krajowym systemie cyberbezpieczeństwa, podmiot publiczny realizujący zadanie publiczne zależne od systemu informacyjnego jest obowiązany do wyznaczenia osoby odpowiedzialnej za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa.

We wszystkich 24 urzędach zostały wyznaczone osoby odpowiedzialne za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa w zakresie związanym z realizacją przez urzędy zadań publicznych zależnych od systemu informacyjnego i systemu teleinformacyjnego wraz z przetwarzanymi w nim danymi w postaci elektronicznej. W dwóch urzędach zgłoszenia osoby odpowiedzialnej za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa do Zespołu Reagowania na Incydentu Bezpieczeństwa Komputerowego NASK, dokonano z opóźnieniem wynoszącym 117 dni (Urząd Miejski w Oławie) i 317 dni (Urząd Miejski w Świeciu), tj. z naruszeniem 14 dniowego terminu określonego w art. 22 ust. 1 pkt 5 ww. ustawy.

Wyznaczenie osób odpowiedzialnych za bezpieczeństwo informacji i ciągłość działania

Tylko w dwóch urzędach[23] nie wyznaczono osób odpowiedzialnych za bezpieczeństwo informacji i ciągłość działania. W pozostałych 22 kontrolowanych urzędach zadania takie powierzono m.in. informatykom, IOD, sekretarzowi powiatu.

---

[21] Dotyczy to starostw w: Lubinie, Sochaczewie i Sępólnie Krajeńskim oraz UM/UG: Koronowo, Nowa Ruda, Sośnicowice, Świętochłowice, Świecie.

[22] Komunikat Ministra Rozwoju i Finansów z dnia 12 grudnia 2016 r. w sprawie standardów audytu wewnętrznego dla jednostek sektora finansów publicznych. (Dz. Urz. MRiF poz. 28).

[23] UM w Sośnicowicach i UM w Świętochłowicach.

Zapewnienie ciągłości działania systemów informatycznych

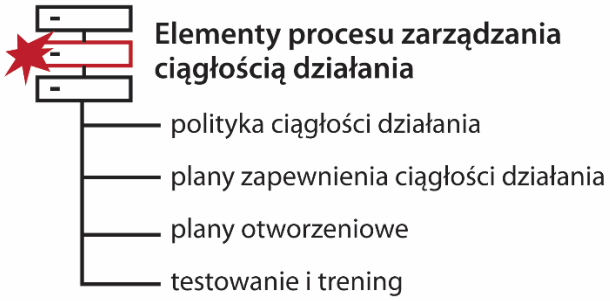
Jak wskazuje Norma ISO 22301:2020-04 *Bezpieczeństwo i odporność. Systemy zarządzania ciągłością działania. Wymagania*, analiza ryzyka w związku z potrzebą zachowania ciągłości działania jest kluczowa. Ciągłość działania to zdolność urzędu do takiego reagowania na zakłócenia warunków normalnej działalności, aby tam, gdzie to możliwe, szybko przywrócić normalne warunki, a tam, gdzie to niemożliwe, przejść do zaplanowanego sposobu zastępczego wykonywania zadań. Ciągłość działania powinna być postrzegana, zarówno w kontekście zadań urzędu oraz procesów służących realizacji tych zadań, jak i poprzez czynniki mogące zakłócić te procesy oraz w kontekście podatności urzędu na zagrożenia, co stanowi o wrażliwości na zakłócenia ciągłości działania.
Zapewnianie ciągłości działania obejmuje ustanowienie mechanizmu reagowania na zakłócenia, proces rozwijania ww. mechanizmu zdolności reagowania na zakłócenia, proces zarządzania bieżącą zdolnością zapewniania ciągłości działania oraz jej stałym doskonaleniem.
Na mechanizm reagowania na zakłócenia składają się:

- struktura organizacyjna urzędu przewidziana do zadania zapewniania ciągłości, stanowiąca spójną całość z ogólną struktura organizacyjną,
- formalne uregulowania organizacyjne określające relacje w strukturze organizacyjnej związane z zadaniem zapewniania ciągłości,
- utrwalona praktyka (możliwie spisana) postępowania w sytuacjach, gdy wymagana jest reakcja na zaistniałe zakłócenie.

Ocena ryzyka, dotycząca zarządzania ciągłością działania, określa prawdopodobieństwo i wpływ zagrożeń, mogących być przyczyną przerwania działalności.

Na infografice nr 3 przedstawiono elementy procesu zarządzania ciągłością działania.

Infografika nr 3



Źródło: opracowanie własne NIK na podstawie wyników kontroli.

Prowadzenie analiz ryzyka w związku z potrzebą zachowania ciągłości działania systemów informatycznych

Ustalono, że w 18 urzędach prowadzone były analizy ryzyka w związku z potrzebą zachowania ciągłości działania systemów informatycznych, z tym że w jednym urzędzie[24] były prowadzone nierzetelnie. W pozostałych sześciu urzędach[25] analizy takie nie były prowadzone, co było działaniem nierzetelnym.

[24] UM Oława.
[25] Dotyczy to starostw w: Kłodzku, Ostrołęce i Sochaczewie oraz UM/UG: Otwock, Osie, Szydłowiec.

Przykłady

W **Urzędzie Miasta Józefowa**, w związku z potrzebą zapewnienia ciągłości działania systemów informatycznych w urzędzie w dniu 10 stycznia 2024 r. Referat Informatyki opracował *Rejestr ryzyk*, w którym wskazano m.in. zidentyfikowane ryzyka, czynniki ryzyka, zastosowane środki kontroli ryzyka, prawdopodobieństwa wystąpienia ryzyka oraz ich skutki, a także prawdopodobieństwo ich wystąpienia i określono reakcje na ryzyko. W dniu 4 stycznia 2024 r. zastępca burmistrza wraz z Inspektor Ochrony Danych Osobowych w Urzędzie opracowali *Analizę zagrożeń i ryzyka przy przetwarzaniu danych osobowych*, w której zawarto m.in. prawdopodobieństwo wystąpienia zagrożenia, przykładowe zagrożenia, skutki naruszenia, sposoby postępowania z ryzykiem, jak również zalecenia dotyczące zminimalizowania ryzyka wystąpienia braku ciągłości działania systemów informatycznych w urzędzie. Burmistrz wyznaczył w urzędzie osoby odpowiedzialne za wdrożenie zaleceń IOD oraz monitorowanie zagrożeń.

W **Urzędzie Miejskim w Głogowie**, w okresie objętym kontrolą w urzędzie prowadzone były coroczne analizy ryzyka w związku z potrzebą zachowania ciągłości działania systemów informatycznych. Analizy te wykonywane były w ramach analiz ryzyka utraty integralności, dostępności lub poufności informacji, a jej wyniki w zakresie zapewnienia ciągłości działania wykorzystano przy tworzeniu i aktualizacji planu ciągłości działania. Prowadzona analiza poprzedzona była inwentaryzacją krytycznych zasobów informatycznych, a następnie określono dla nich listę obejmującą 51 zagrożeń/ryzyk z podziałem na zewnętrzne i wewnętrzne. Dla tak zdefiniowanych ryzyk określano prawdopodobieństwo ich wystąpienia oraz skutek ich zmaterializowania oraz proponowano sposób postępowania w celu ich zmniejszenia lub ograniczenia. Dokument taki był przekazywany sekretarzowi i podlegał akceptacji przez prezydenta.

Ustanowienie polityk ciągłości działania

W 17 kontrolowanych urzędach[26] (71 %) nie ustanowiono polityk ciągłości działania, co było nierzetelne. Celem Polityki ciągłości działania jest określenie założeń, zakresu oraz podstawowych zasad zarządzania ciągłością działania. Określenie polityki ciągłości działania służy zdefiniowaniu zaleceń, których celem jest zapewnienie funkcjonowania krytycznych procesów w sytuacji kryzysowej. Brak ustanowienia polityki ciągłości działania w urzędach negatywnie wpływa na ich przygotowanie na sytuacje awaryjne, istotnie utrudniając skuteczne reagowanie na ich wystąpienie i zapewnienie ciągłego działania.

Na infografice nr 4 przedstawiono udział procentowy urzędów, w których nie ustanowiono polityki ciągłości działania.

[26] Dotyczy to starostw w: Kłodzku, Ostrołęce, Sępólnie Krajeńskim i Sochaczewie oraz UM/UG: Czechowice-Dziedzice, Józefów, Kcynia, Oława, Otwock, Osie, Nowa Ruda, Pyskowice, Sośnicowice, Szydłowiec, Świętochłowice, Zbrosławice, Żyrardów.

Infografika nr 4

Źródło: opracowanie własne NIK na podstawie wyników kontroli.

Opracowanie i wdrożenie Planów zapewnienia ciągłości działania oraz Planów odtworzeniowych

Strategia odtworzenia dla poszczególnych działań określona jest w utworzonych planach ciągłości/odtworzenia działania. Plan ciągłości i odtworzenia działania w szczególności będzie dotyczył m.in.:

- zasilania i topologii sieci,
- klastrów i macierzy dyskowych,
- systemów kopii zapasowych,
- systemowych serwerów wirtualnych,
- urządzeń brzegowych.

W planach takich określa się tzw. akceptowalny czas przywrócenia do działania rozumiany jako czas określony przez urząd w jakim nastąpi ponowne uruchomienie systemów informatycznych niezbędnych do funkcjonowania urzędu.

W 12 kontrolowanych urzędach[27] (50 %) nie opracowano Planów zapewnienia ciągłości działania oraz Planów odtworzeniowych, co było nierzetelne.

Przykład

W **Starostwie Powiatowym w Sochaczewie** wskazano, że plany *nie zostały opracowane na piśmie. (...) Testowanie, nie zostało przeprowadzone. Taki stan rzeczy jest wynikiem braku posiadania sprzętu jaki można do takiej symulacji wykorzystać, brak urządzeń zapasowych o parametrach takich samych jak posiadane lub lepszych. (...) Akceptowalny czas przywrócenia ciągłości działania systemów informatycznych nie został określony w sposób dokładny z powodu braku możliwości przetestowania takiej sytuacji, z uwagi na brak sprzętu zapasowego. W przybliżeniu takie działanie zajęłoby ok. 24 h w momencie posiadania identycznego lub lepszego sprzętu jaki jest obecnie na wyposażeniu Urzędu*.

Testowanie Planów ciągłości działania oraz Planów odtworzeniowych

Jak wskazuje Norma ISO 22301 w przypadku Planu zapewnienia ciągłości działania oraz Planów odtworzeniowych istotne jest ich cykliczne testowanie w celu uzyskania potwierdzenia, że w sytuacji wystąpienia incydentu ciągłości działania zadziałają one prawidłowo. Nie jest możliwe zasymulowanie w pełni zaistniałej katastrofy, np. zalanie, pożar budynku, dlatego też plany te są

[27] Dotyczy to starostw w: Kłodzku, Ostrołęce, Sochaczewie i Wąbrzeźnie oraz UM/UG: Józefów, Kcynia, Koronowo, Oława, Otwock, Sośnicowice, Szydłowiec, Świętochłowice.

testowane jedynie w możliwym zakresie. Istotne jest zidentyfikowanie słabych punktów tych planów w trakcie ćwiczeń. W ćwiczeniach tych powinni brać udział wszyscy zaangażowani w daną działalność pracownicy. Wszystkie działania w tym zakresie winny być dokumentowane.

Spośród 12 urzędów, w których opracowano Plany zapewnienia ciągłości działania oraz Plany odtworzeniowe tylko w pięciu urzędach[28] były one testowane.

Przykład

Obowiązujący w **Urzędzie Miejskim w Głogowie** Plan ciągłości działania nakładał obowiązek przeprowadzania jego testowania przynajmniej raz na 24 miesiące, mając na celu sprawdzenie jego aktualności. Z czynności takiej należało złożyć raport sekretarzowi. W okresie objętym kontrolą, w dniach od 2 do 24 października 2023 r., przeprowadzono i udokumentowano testy planu ciągłości działania oraz sprawdzenie jego aktualności, a raport z tych działań przedłożono sekretarzowi.

5.2. PRAWIDŁOWOŚĆ, RZETELNOŚĆ I SKUTECZNOŚĆ WDROŻENIA PRZYJĘTYCH ROZWIĄZAŃ ORGANIZACYJNYCH I TECHNICZNYCH, TJ. CZY SĄ ONE FAKTYCZNIE STOSOWANE I EGZEKWOWANE

Wdrożone rozwiązania w zakresie bezpieczeństwa informacji nie zawsze były właściwie stosowane i egzekwowane

W większości urzędów (83 %) nie wszystkie wdrożone rozwiązania organizacyjne i techniczne w zakresie bezpieczeństwa informacji były właściwie egzekwowane. W 20 podmiotach (83 %) wystąpiły nieprawidłowości w zakresie: zabezpieczenia serwerowni, sporządzania kopii zapasowych, braku w umowach na zakup usług IT lub serwis sprzętu/oprogramowania odpowiednich zapisów w zakresie bezpieczeństwa informacji, co stanowiło naruszenie obowiązków wynikających z obowiązującego rozporządzenia KRI. W 18 urzędach (75 %) nie w pełni przestrzegano ustanowionych zasad dostępu do systemów informatycznych oraz nie zawsze zidentyfikowano kluczowe elementy infrastruktury i usług IT (37 % urzędów). Ponadto, w 21 urzędach (83 %) nie monitorowano telefonów służbowych oraz tabletów.

Zarządzanie uprawnieniami pracowników w systemach informatycznych urzędów

W trakcie kontroli ustalono, że 11 spośród 235 pracowników objętych badaniem wykonujących zadania w systemach informatycznych (tj. 5 %), miało możliwość zainstalowania na użytkowanych komputerach dowolnego oprogramowania. Sytuacja taka wystąpiła w czterech urzędach[29] (tj. w 17 %). W jednym urzędzie[30] wszyscy badani użytkownicy systemów informatycznych niebędący pracownikami służb informatycznych posiadali uprawnienia administratora systemu na używanych przez nich komputerach, w związku z czym mogli samodzielnie instalować dowolne oprogramowanie. Było to niezgodne z wymaganiami określonymi w § 19 ust. 2 pkt 4 obowiązującego rozporządzenia KRI. W trakcie kontroli NIK odbierano tym pracownikom uprawnienia administratora.

[28] Dotyczy to starostwa w Lubinie oraz UM/UG: Głogów, Kamienna Góra, Sośnicowice, Zbrosławice.

[29] Urząd (liczba badanych użytkowników/liczba użytkowników posiadających uprawnienia administratora): Starostwo Powiatowe w Kłodzku (5/5), Starostwo Powiatowe w Sępólnie Krajeńskim (13/1), Urząd Miasta Otwocka (10/1), Urząd Gminy w Osiu (10/4).

[30] Starostwo Powiatowe w Kłodzku.

W wyniku badania przyznanych uprawnień dostępu do korzystania z systemów informatycznych, dokonanego na łącznej próbie 359 pracowników kontrolowanych urzędów, stwierdzono że w przypadku ośmiu osób[31] nadane uprawnienia były nieadekwatne do zadań określonych w zakresach czynności tych osób. Było to niezgodne z § 19 ust. 2 pkt 4 obowiązującego rozporządzenia KRI, stanowiącego że zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienie przez kierownictwo podmiotu publicznego warunków umożliwiających realizację i egzekwowanie m.in. podejmowania działań zapewniających, że osoby zaangażowane w proces przetwarzania informacji posiadają stosowne uprawnienia i uczestniczą w tym procesie w stopniu adekwatnym do realizowanych przez nie zadań oraz obowiązków.

W wyniku przeprowadzonego badania blokowania lub odbierania dostępu do systemów informatycznych na próbie 240 osób, które zakończyły zatrudnienie w kontrolowanych urzędach, stwierdzono, iż 52 byłym pracownikom (tj. 22 %) 15 urzędów[32] konta nie zostały zablokowane i pozostawały wciąż aktywne. Było to niezgodne z § 19 ust. 2 pkt 5 obowiązującego rozporządzenia KRI, stanowiącym że zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienie przez kierownictwo podmiotu publicznego warunków umożliwiających realizację i egzekwowanie bezzwłocznej zmiany uprawnień, w przypadku zmiany zadań osób zaangażowanych w proces przetwarzania informacji. Zakres nieodebranych uprawnień, jak i okres po jakim zablokowano dostęp do kont, był w poszczególnych urzędach zróżnicowany.

Przykład

W **Urzędzie Miasta Otwocka** stwierdzono, że według stanu na dzień 3 lipca 2024 r. wszystkie 10 osób, które w okresie od 1 stycznia 2023 r. do 3 czerwca 2024 r. zakończyły zatrudnienie w urzędzie, nadal posiadały aktywne konta w systemie informatycznym EZD. Ponadto ustalono, że w przypadku czterech z 10 osób, ich konta w domenie Urzędu były nadal aktywne (nie były zablokowane ani usunięte), oraz że nadal aktywne było konto jednego pracownika wykonującego zadania w systemie Groszek UmowyFV. Brak usunięcia/zablokowania kont wynikał, jak wyjaśniano, z niedopatrzenia. Prezydent Miasta Otwocka podał ponadto, że *analiza sytuacji wykazała, że (...) konta zostały odblokowane i zmienione zostały hasła w celu uzyskania dostępu do plików służbowych na potrzebę ich przełożonych. Nie określono terminu ponownej blokady tych kont*. Odnośnie systemu EZD, Prezydent wyjaśnił, że *praktyką przyjętą przez Wydział Informatyki w celu zablokowania dostępu do EZD była zmiana hasła. Wynikło to przyjętych zwyczajów przekazanych przez byłych pracowników Wydziału Informatyki. W wyniku bieżącej kontroli odnaleziono i zastosowano w EZD funkcję blokowania użytkowników.*

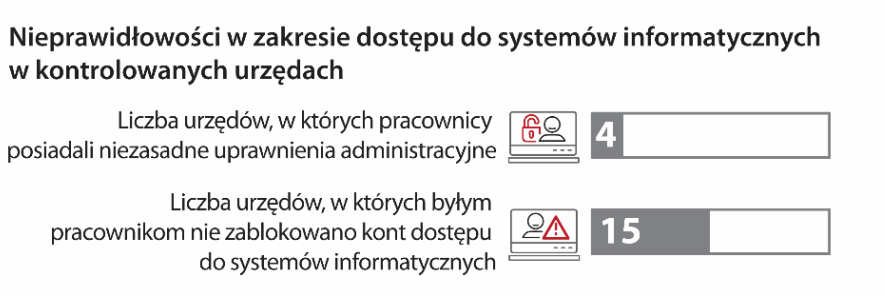
[31] Dotyczy Starostw Powiatowych w: Ostrołęce (cztery osoby), Sępólnie Krajeńskim (jedna osoba), Urzędu Miasta Żyrardowa (jedna osoba) i Urzędu Miejskiego w Sośnicowicach (jedna osoba) i Urzędu Gminy Zbrosławice (jedna osoba).

[32] Starostwa Powiatowe w: Ostrołęce (cztery osoby), Sochaczewie (dwie osoby), Sępólnie Krajeńskim (dwie osoby), Wąbrzeźnie (jedna osoba), Lubinie (pięć osób) oraz w UM/UG: Józefów (jedna osoba), Otwock (dziesięć osób), Szydłowiec (jedna osoba), Kcynia (cztery osoby), Koronowo (dwie osoby), Czechowice-Dziedzice (jedna osoba), Zbrosławice (siedem osób), Kamienna Góra (osiem osób), Oława (dwie osoby), Nowa Ruda (dwie osoby).

Odnośnie kont w domenie urzędu, NIK zauważa, że funkcjonalność wykorzystywanego w urzędzie mechanizmu Microsoft Active Directory pozwala na dostęp do plików służbowych byłych pracowników z poziomu administratora bez konieczności odblokowania kont tych pracowników. W związku z tym konta byłych pracowników powinny być zablokowane.

Nieprawidłowości w zakresie dostępu do systemów informatycznych przedstawiono na infografice nr 5.

Infografika nr 5



Źródło: opracowanie własne NIK na podstawie wyników kontroli.

Zabezpieczenia techniczne i wymogi w systemach informatycznych zapewniające ochronę informacji i ich przestrzeganie w praktyce

We wszystkich kontrolowanych urzędach w celu zapewnienia ochrony przetwarzanych informacji przed nieuprawnionym dostępem wprowadzono zabezpieczenia polegające m.in. na konieczności logowania się do systemów informatycznych z wykorzystaniem unikalnego identyfikatora oraz hasła o odpowiedniej złożoności. Wymogi dotyczące zasad dostępu do systemów informatycznych określane były w uregulowaniach wewnętrznych urzędów, w tym m.in. w Polityce Bezpieczeństwa Informatycznego i Instrukcji Zarządzania Systemem Informatycznym.

Przykład

W wyniku oględzin trzech systemów informatycznych zarządzanych przez **Urząd Miejski w Szydłowcu** stwierdzono, że wprowadzono w nich zabezpieczenia techniczne w celu zapewnienia ochrony przetwarzanych informacji przed nieuprawnionym dostępem. W tym celu w systemach informatycznych urzędu wykorzystywano identyfikatory użytkowników oraz hasła dostępu o odpowiedniej złożoności. Złożoność hasła polegała na ustanowieniu wymogu wprowadzenia przez użytkownika systemu informatycznego ciągu znaków o określonej długości i złożoności. Oględziny trzech systemów informatycznych zarządzanych przez urząd pod kątem wymagań dla haseł dostępu do tych systemów wykazały, że wymogi w zakresie złożoności (siły) haseł oraz okresów po jakim hasło powinno być zmienione zostały zachowane. Zweryfikowane w toku oględzin systemy informatyczne wykorzystywane w urzędzie umożliwiały realizację tych wymogów. W urzędzie komputery z systemem operacyjnym Windows były zarządzane centralnie w oparciu o mechanizm *Microsoft Active Directory*. Na podstawie listy identyfikatorów użytkowników ww. trzech badanych systemów pod kątem loginów ustalono, że nazwa pozwala na bezpośrednie powiązanie ich z daną osobą[33]. W trakcie oględzin nie stwierdzono, żeby na dane konto mogło zalogować się kilka osób.

[33] Login powstał od połączenia pierwszych liter imienia i nazwiska użytkownika.

Pomimo ustanowienia wymogów w zakresie uzyskiwania dostępu do systemów informatycznych, w dziewięciu kontrolowanych urzędach (37 %) zasady te nie były w pełni przestrzegane[34]. Nieprawidłowości w tym zakresie dotyczyły przede wszystkim stosowania przez użytkowników haseł do systemów informatycznych krótszych niż wymagane. Ponadto, w urzędach tych nie korzystano z istniejącej w systemach dziedzinowych funkcji, która wymusza stosowanie zasad dotyczących złożoności haseł ustanowionych w urzędzie.

Przykład

W **Urzędzie Miejskim w Nowej Rudzie**, trzy poddane sprawdzeniu systemy informatyczne użytkowane przez urząd nie wymuszały zmiany hasła i jego złożoności, co było niezgodne z pkt 6 polityki haseł ustanowionej w urzędzie. Umożliwiało to stosowanie nieadekwatnych haseł dostępu do tych systemów w odniesieniu do istotności zawartych w nich informacji i było niezgodne z § 19 ust. 2 pkt 7 lit. c obowiązującego rozporządzenia KRI. Informatyk wyjaśnił, że nadawał stałe hasła każdemu użytkownikowi i nie posiadał wiedzy czy użytkownik dokonał zmiany hasła i w jakim zrobił to terminie. Dodał również, że niezwłocznie zostanie połączone logowanie do modułów systemów z usługą Active Directory, co spowoduje automatyzację zmiany haseł w wymaganym okresie przez użytkowników systemów. Nieprawidłowość ta została usunięta w trakcie trwania kontroli.

Zapobieganie wglądowi w dane osobowe wyświetlane na monitorach

Z przeprowadzonych w trakcie kontroli oględzin w 24 kontrolowanych urzędach na łącznie 117 stanowiskach komputerowych wynika, że w dwóch urzędach[35] łącznie trzy monitory usytuowane były w sposób umożliwiający wgląd do danych przez osoby nieuprawnione. Monitory znajdowały się w pomieszczeniach, w których obywatele załatwiali sprawy urzędowe, np. związane z wydawaniem dowodu osobistego lub rejestracją pojazdu, wydaniem prawa jazdy.

Ustanowienie zasad pracy przy przetwarzaniu mobilnym i pracy na odległość

W trzech urzędach[36] (12 %) nie określono szczegółowych zasad i procedur korzystania przez pracowników z urządzeń przenośnych poza jego siedzibą, gwarantujących bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość, co było niezgodne z § 19 ust. 2 pkt 8 obowiązującego rozporządzenia KRI. Kontrolowani wskazywali, że wykorzystywanie komputerów przenośnych poza siedzibą urzędu nie występuje, stąd nie było potrzeby ustanowienia procedur w tym zakresie.

Zabezpieczenie danych na urządzeniach mobilnych

Biorąc pod uwagę możliwość wynoszenia sprzętu informatycznego poza siedzibę urzędu wskazane jest zastosowanie rozwiązania polegającego na szyfrowaniu dysków twardych komputerów przenośnych, dzięki czemu, w przypadku ich kradzieży lub zagubienia, osoby postronne nie będą miały dostępu do danych na nich zgromadzonych.

Badanie w zakresie stosowania rozwiązania polegającego na szyfrowaniu dysków twardych komputerów przenośnych wykazało, że w trzech z 24 kontrolowanych urzędów[37] (12 %) nie stosowano takich rozwiązań,

[34] Starostwa Powiatowe w: Lubinie i Sępólnie Krajeńskim, UM/UG: Józefów, Kamienna Góra, Kcynia, Nowa Ruda, Osie, Otwock, Zbrosławice.
[35] UM/UG: Józefów i Otwock.
[36] Starostwa Powiatowe w: Ostrołęce i Sępólnie Krajeńskim oraz UG Osie.
[37] Starostwa Powiatowe w: Sępólnie Krajeńskim i Sochaczewie oraz UG Osie.

co było niezgodne z § 19 ust. 2 pkt 9 i 11 obowiązującego rozporządzenia KRI. Szyfrowanie danych zgromadzonych na urządzeniach mobilnych jest dobrą praktyką pozwalającą na zachowanie poufności informacji w przypadku utraty (zagubienia, kradzieży) urządzenia mobilnego.

Stan zabezpieczenia danych na urządzeniach mobilnych urzędów jst przedstawiono w infografice nr 6.

Infografika nr 6

Źródło: opracowanie własne NIK na podstawie wyników kontroli.

Monitorowanie komórkowych telefonów służbowych/tabletów

Jedynie w trzech urzędach[38] wprowadzono rozwiązania techniczne umożliwiające monitorowanie oprogramowania wykorzystywanego na telefonach służbowych/tabletach. W pozostałych 21 kontrolowanych urzędach nie wprowadzono rozwiązań technicznych do monitorowania komórkowych telefonów służbowych/tabletów. Kontrolowani wskazywali m.in., że telefony służbowe nie były podłączane do żadnych wewnętrznych systemów informatycznych urzędu. Telefony, które były podłączane do sieci bezprzewodowej w celu dostępu do Internetu, korzystały wyłącznie z odseparowanej logicznie sieci gościnnej. Do sieci wewnętrznej miały dostęp tylko monitorowane i zabezpieczone służbowe komputery/laptopy. Telefony były traktowane jako urządzenia zewnętrzne, które służyły pracownikom do komunikacji.

Zdaniem NIK, oprogramowanie instalowane na urządzeniach mobilnych (telefony służbowe/tablety) nie powinno pozostawać poza nadzorem. Urząd powinien zapewnić rozwiązania techniczne do monitorowania oprogramowania na tych urządzeniach.

Niewystarczające zabezpieczenia serwerowni w połowie urzędów

W 12 urzędach[39] (50 %) zastosowano zabezpieczenia fizyczne serwerowni, które w niewystarczającym stopniu chroniły te pomieszczenia. Było to niezgodne z § 19 ust. 2 pkt 9 obowiązującego rozporządzenia KRI, stanowiącego że zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienie przez kierownictwo podmiotu publicznego warunków umożliwiających realizację i egzekwowanie m.in. zabezpieczenia informacji w sposób uniemożliwiający nieuprawnionemu jej ujawnienie, modyfikację, usunięcie lub zniszczenie. Ponadto, wskazane

[38] UM/UG: Kamienna Góra, Pyskowice i Sośnicowice.

[39] Starostwa Powiatowe w: Kłodzku, Lubinie, Ostrołęce, Sochaczewie, Wodzisławiu Śląskim oraz UM/UG: Czechowice-Dziedzice, Kamienna Góra, Nowa Ruda, Oława, Otwock, Osie, Świętochłowice.

jest aby w celu ochrony sprzętu wprowadzić zabezpieczenia minimalizujące ryzyko związane z potencjalnymi zagrożeniami fizycznymi i środowiskowymi, np. kradzieżą, pożarem, dymem, zalaniem.

Zapewnienie bezpieczeństwa informacji w umowach z podmiotami zewnętrznymi

Przepis § 19 ust. 2 pkt 10 obowiązującego rozporządzenia KRI zobowiązuje do zawierania w umowach serwisowych podpisanych ze stronami trzecimi zapisów gwarantujących odpowiedni poziom bezpieczeństwa informacji.

Kontrola wykazała, że w 11 urzędach (46 %) w umowach na zakup usług informatycznych, zakup lub serwis sprzętu komputerowego/oprogramowania stwierdzono brak zapisów gwarantujących zabezpieczenie poufności informacji uzyskanych przez wykonawców w związku z realizacją tych umów, co było niezgodne z § 19 ust. 2 pkt 10 obowiązującego rozporządzenia KRI. Zapisów takich nie zawarto łącznie w 30 umowach[40] spośród 101 objętych badaniem (tj. 30 %).

Kontrolowani podawali m.in., że w umowach zawarto zapisy dotyczące ochrony danych osobowych, co w ich opinii było wystarczające.

Zdaniem NIK, zobowiązanie wykonawców umów wyłącznie do ochrony danych osobowych jest niewystarczające. W zawieranych umowach powinny być klauzule gwarantujące urzędowi zachowanie w tajemnicy wszelkich informacji do jakich wykonawca może mieć dostęp w związku z realizacją umowy.

Przykład

W **Starostwie Powiatowym w Sochaczewie**, w przypadku ośmiu umów nie zawarto w nich *zapisów gwarantujących odpowiedni poziom bezpieczeństwa informacji*. Sekretarz powiatu wyjaśnił, że w przypadku umów o świadczenie usług informatycznych na rzecz starostwa *nie zawarto klauzuli zapewniającej bezpieczeństwo informacji. Z osobami, które obecnie świadczą obsługę informatyczną w ramach zawartych umów zostały podpisane upoważnienia do przetwarzania danych osobowych, w których znajduje się oświadczenie osoby upoważnionej w którym (...) zobowiązuję się do zachowania poufności, nieujawniania osobom nieupoważnionym i zachowania w tajemnicy wszelkich danych, z którymi ma styczność podczas wykonywania zadań służbowych lub będzie mieć dostęp, a nie przeznaczonych do publicznego rozpowszechniania.*

W pozostałych kontrolowanych 13 urzędach umowy na zakup usług informatycznych, zakup lub serwis sprzętu komputerowego/oprogramowania zawierały zapisy o zobowiązaniu wykonawców umów do zachowania w tajemnicy informacji, do jakich mogą mieć dostęp w związku z realizacją umowy.

[40] Starostwa Powiatowe w (liczba umów bez właściwych zapisów/liczba zbadanych umów): Lubinie (1/4), Ostrołęce (3/4), Sępólnie Krajeńskim (2/4), Sochaczewie (8/12) i Wąbrzeźnie (4/4) oraz UM/UG: Józefów (2/4), Kamienna Góra (2/4), Kcynia (1/3), Oława (2/4), Osie (4/4), Sośnicowice (1/2).

Tworzenie, przechowywanie i testowanie kopii zapasowych

Zgodnie z wymogami określonymi w § 19 ust. 2 pkt 12 lit. b obowiązującego rozporządzenia KRI, zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienie przez kierownictwo podmiotu publicznego warunków umożliwiających realizację i egzekwowanie m.in. zapewnienia odpowiedniego poziomu bezpieczeństwa w systemach teleinformatycznych, polegającego w szczególności na minimalizowaniu ryzyka utraty informacji w wyniku awarii.

W 12 urzędach (50 %) stwierdzono nieprawidłowości polegające na niespełnieniu wymogów wynikających z § 19 ust. 2 pkt 12 lit. b obowiązującego rozporządzenia KRI, które polegały na:

- niewłaściwym przechowywaniu kopii zapasowych danych z systemów informatycznych, tj. w sposób, który nie minimalizuje ryzyka utraty informacji i stwarza zagrożenie, że w przypadku zdarzeń losowych. W razie np. pożaru lub zalania, urząd może utracić zarówno dane źródłowe, jak i ich kopie zapasowe. W siedmiu urzędach[41] (29 %) stwierdzono, że sporządzane kopie zapasowe przechowywane były w serwerowniach, a więc w miejscach wytwarzania danych, albo w miejscu, do którego dostęp miały osoby nieupoważnione. Kopie zapasowe powinny być przechowywane w innej lokalizacji, w odległości pozwalającej uniknąć uszkodzeń spowodowanych katastrofą, która dotknęła ośrodek podstawowy;
- niesporządzaniu kopii zapasowych lub tworzono je niezgodnie z przyjętymi procedurami (w trzech urzędach[42]);
- braku testowania kopii zapasowych w sześciu urzędach[43]. Nośniki kopii zapasowych powinny być testowane aby można było na nich polegać w przypadku awaryjnego odtwarzania.

W pozostałych 12 kontrolowanych urzędach (50 %) kopie zapasowe danych były właściwie tworzone, przechowywane oraz testowane.

Monitorowanie pojemności nośników pamięci systemów informatycznych

W większości kontrolowanych urzędów (21 z 24) nie przyjęto formalnej procedury monitorowania pojemności nośników pamięci masowych, wykorzystywanych w serwerach. Monitoring taki był prowadzony ręcznie przez informatyków.

Przykład

Procedury obowiązujące w **Starostwie Powiatowym w Kłodzku** nie przewidywały monitorowania pojemności nośników pamięci serwerów, natomiast w praktyce cały proces monitoringu był realizowany przez oprogramowanie, które było w posiadaniu urzędu. Równocześnie w trakcie kontroli NIK w oprogramowaniu służącym do inwentaryzacji sprzętu IT uruchomiono funkcjonalność dotyczącą monitorowania i informowania pracowników o przepełnieniu dyskowym.

[41] Starostwo Powiatowe w Sochaczewie oraz UM/UG: Józefów, Kamienna Góra, Kcynia, Nowa Ruda, Szydłowiec, Zbrosławice.
[42] Starostwo Powiatowe w Sępólnie Krajeńskim oraz UM/UG: Czechowice-Dziedzice i Osie.
[43] Starostwa Powiatowe w: Sępólnie Krajeńskim, Sochaczewie i Wąbrzeźnie oraz UM/UG: Kcynia, Osie, Świecie.

Starostwo posiadało na stanie pięć serwerów fizycznych i 10 wirtualnych. Przeprowadzony w toku oględzin test zajętości trzech serwerów wykazał poszczególne zajętości, które wynosiły: Serwer 1– zajętość 29 %; Serwer 2 – zajętość 40 %; Serwer 3 – zajętość 78 %.

W trzech urzędach[44] oględziny zapełnienia przestrzeni dyskowych wybranych do badania serwerów wykazały, że zajętość partycji przeznaczonej na dane przekraczała 80 %, co zdaniem NIK mogło wpływać na wydajność pracy systemów informatycznych urzędu.

NIK wskazuje, że zajętość przestrzeni dyskowej powinna być stale monitorowana w celu dostosowywania wykorzystania zasobów oraz przewidywania wymaganej pojemności w przyszłości oraz nie powinna przekraczać 80 % dla zapewnienia właściwej wydajności systemu i aplikacji.

Identyfikacja kluczowych elementów infrastruktury i usług IT w celu zapewnienia ciągłości działania

W ramach zapewnienia ciągłości działania, w sposób udokumentowany, w dziewięciu kontrolowanych urzędach[45] (37 %) nie zidentyfikowano kluczowych elementów infrastruktury i usług IT oraz nie ustalono ich zabezpieczenia pod kątem wpływu czynników zewnętrznych. Zarządzanie ciągłością działania ma na celu zapewnienie, że infrastruktura i usługi IT będą mogły być odtworzone do wcześniej zdefiniowanych poziomów. Dlatego też istotne jest zidentyfikowanie kluczowych dla pracy urzędu elementów infrastruktury informatycznej, jak i usług informatycznych. Bez zdefiniowania tych kwestii nie jest możliwe szybkie i skuteczne przywrócenie infrastruktury i usług IT w sytuacji wystąpienia zakłócenia ciągłości działania.

W pozostałych 15 urzędach prowadzono działania, w ramach których zidentyfikowano kluczowe elementy infrastruktury i usług IT niezbędne dla zapewnienia ciągłości działania systemów informatycznych.

Przykład

W **Starostwie Powiatowym w Lubinie** w ramach zapewnienia ciągłości działania urzędu zidentyfikowano kluczowe elementy infrastruktury IT oraz kluczowe usługi IT, wykorzystywane w jednostce. Identyfikacja ta dokonywana była corocznie jako element szacowania ryzyka aktywów informacyjnych. W dokumentacji ciągłości działania nie wskazano czasu przywrócenia poszczególnych systemów oraz procesów do działania. W złożonych wyjaśnieniach sekretarz powiatu stwierdził, że dokładne określenie czasu przywrócenia poszczególnych systemów oraz procesów do działania jest niezwykle trudne, m.in. z powodu warunków w jakich proces ten będzie przeprowadzany; wielkości zasobów przyrastających z dnia na dzień oraz aktualizacji dostarczanych przez zewnętrznych dostawców.

[44] Starostwo Powiatowe w: Sępólnie Krajeńskim oraz UM/UG: Koronowo i Osie.

[45] Starostwa Powiatowe w: Kłodzku, Ostrołęce i Sępólnie Krajeńskim oraz UM/UG: Czechowice-Dziedzice, Kcynia, Nowa Ruda, Osie, Otwock, Świecie.

5.3. CYKLICZNE PODEJMOWANIE DZIAŁAŃ MAJĄCYCH NA CELU ZAPOBIEGANIE INCYDENTOM BEZPIECZEŃSTWA INFORMACJI (SZKOLENIA, ANALIZA INCYDENTÓW, AUDYTY, ANALIZA RYZYKA)

Urzędy w ograniczonym zakresie podejmowały działania mające na celu zapobieganie incydentom bezpieczeństwa informacji

Kontrolowane urzędy w ograniczonym zakresie podejmowały działania mające na celu zapobieganie incydentom bezpieczeństwa informacji. Wprawdzie w 17 urzędach (71 %) prowadzono okresowe analizy ryzyka utraty integralności, poufności, dostępności informacji oraz w 20 urzędach (83 %) wdrożone były procedury wewnętrzne zgłaszania i obsługi incydentów naruszenia bezpieczeństwa informacji, jednak w dziesięciu urzędach (42 %) nie przeprowadzono szkoleń pracowników z zakresu bezpieczeństwa informacji, a w dziewięciu urzędach (37 %) wystąpiły nieprawidłowości w zakresie okresowego audytu bezpieczeństwa informacji.

Okresowe analizy ryzyka utraty integralności, poufności lub dostępności informacji

W celu skutecznego zaprojektowania Systemu Zarzadzania Bezpieczeństwem Informacji konieczne 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 i jest zależny od istotności informacji podlegających ochronie będących w posiadaniu lub przetwarzaniu urzędu. Rodzaj zastosowanych zabezpieczeń technicznych, jak i ich poziom wynika zatem z szacowania ryzyka. Proces zarządzania ryzykiem składa się z następujących etapów: identyfikacja ryzyka, analiza ryzyka, w tym określenie poziomu ryzyka, ocena ryzyka (czy ryzyko jest akceptowalne lub tolerowane, a jeżeli nie, to określenie sposobu postępowania z ryzykiem). Jest to zadanie o charakterze ciągłym.

Biorąc pod uwagę różnorodność i częstotliwość pojawiających się zagrożeń dla zachowania bezpieczeństwa informacji, dobrą praktyką jest aby procedura szacowania ryzyka była przeprowadzana co najmniej raz na rok (lub częściej w przypadku pojawienia się nowych zagrożeń).

W siedmiu urzędach (29 %)[46] nie prowadzono okresowych analiz ryzyka utraty integralności, poufności, dostępności, co było niezgodne z § 19 ust. 2 pkt 3 obowiązującego rozporządzenia KRI lub analizy te nie były właściwie dokumentowane. Jako przyczynę tej nieprawidłowości, kontrolowani wskazywali m.in. na nieprzypisanie tego zadania żadnemu z pracowników urzędu, brak kompetentnych pracowników w tym zakresie, trudną sytuację finansową urzędu.

W pozostałych 17 jednostkach (71 %) przeprowadzenie takiej analizy umożliwiło ustalenie istotnych ryzyk mających wpływ na zapewnienie bezpieczeństwa informacji. Dokonano oceny istotności tych ryzyk oraz podjęto działania w celu zminimalizowania ich wpływu na działalność urzędu.

[46] Starostwa Powiatowe w: Ostrołęce, Sochaczewie oraz UM/UG: Oława, Otwock, Sośnicowice, Świecie, Szydłowiec.

Przykład

Zgodnie z przyjętą w **Urzędzie Miasta Kamienna Góra** *Procedurą zarządzania ryzykiem*, w 2023 r. przeprowadzono w Urzędzie coroczną analizę ryzyka bezpieczeństwa informacji, zatwierdzoną przez Burmistrza 31 października 2023 r. Na ww. analizę składały się: [1] arkusze identyfikacji ryzyka w komórce organizacyjnej, zawierające realizowane przez daną komórkę zadania, zidentyfikowane ryzyka oraz zastosowane środki organizacyjne i techniczne[47] wprowadzone w celu minimalizacji tego ryzyka i utraty bezpieczeństwa informacji oraz [2] arkusze identyfikacji oceny ryzyka bezpieczeństwa informacji w poszczególnych komórkach organizacyjnych urzędu, w których wskazano: realizowane zadania, zidentyfikowane ryzyka z nimi związane, ocenę prawdopodobieństwa i skutku danego ryzyka oraz skalę tego ryzyka, osobę odpowiedzialną za dane ryzyko oraz plan postępowania z danym ryzykiem.

Zgłaszanie incydentów naruszenia bezpieczeństwa informacji oraz incydentów dotyczących danych osobowych

Bezzwłoczne zgłaszanie incydentów z zakresu naruszenia bezpieczeństwa informacji ma na celu zapewnienie szybkiej reakcji i podjęcie odpowiednich działań. Zgodnie z normą PN-ISO/IEC 27001 przez incydent związany z bezpieczeństwem informacji należy rozumieć pojedyncze zdarzenie lub serię niepożądanych albo niespodziewanych zdarzeń związanych z bezpieczeństwem informacji, które stwarzają znaczne prawdopodobieństwo zakłócenia działań biznesowych i zagrażają bezpieczeństwu informacji. Z kolei artykuł 33 RODO reguluje zgłaszanie naruszenia ochrony danych osobowych organowi nadzorczemu.

W okresie objętym kontrolą w 20 urzędach (83 %) wdrożone były procedury wewnętrzne zgłaszania i obsługi incydentów naruszenia bezpieczeństwa informacji, przewidziane w § 19 ust. 2 pkt 13 obowiązującego rozporządzenia KRI. W urzędach tych ustalono także sposób postępowania w przypadku naruszenia ochrony danych osobowych.

Przykład

W **Urzędzie Miejskim w Szydłowcu** procedura w zakresie zgłaszania incydentów naruszenia bezpieczeństwa informacji w urzędzie była opisana w załączniku nr 14 do SZBI. Sposób postępowania w przypadku wystąpienia incydentu naruszenia ochrony danych osobowych został również opisany w przyjętej w ramach Polityki ochrony danych osobowych procedury pn. *Procedura postępowania w sytuacji naruszenia ochrony danych osobowych*[48]. Procedura uwzględniała postanowienia art. 33 i 34 RODO.

[47] Na przykład w przypadku ryzyka zainstalowania złośliwego oprogramowania przez stronę internetową lub użytkowania zewnętrznych nośników, zakłada się regularne aktualizowanie systemu antywirusowego, zabronienie instalowania jakiegokolwiek oprogramowania bez wiedzy ASI. Dodatkowo wdrożono system monitoringu użytkownika komputera, filtr treści FIREWALL, na stacjach roboczych zablokowano wejścia USB, nie można korzystać z zewnętrznych nośników informacji.

[48] Zarządzenie nr 173/2019 Burmistrza Szydłowca z dnia 30 grudnia 2019 r. Ostatnia aktualizacja procedury, wersja nr 3 z dnia 14 czerwca 2023 r.

Zastępca burmistrza poinformowała, że w urzędzie w okresie objętym kontrolą nie odnotowano *ujawnienia informacji osobom nieupoważnionym; udostępnienie hasła i loginu innym użytkownikom, złamania zasad polityki bezpieczeństwa informacji, zablokowania strony internetowej urzędu, podejrzenia kradzieży danych czy też kradzieży systemów (laptop, urządzenie przenośne).*

W okresie objętym kontrolą wystąpiły dwa incydenty bezpieczeństwa informacji. Dotyczyły one systemów zewnętrznych, administrowanych przez podmioty zewnętrzne.

Zastępca burmistrza wyjaśniła, że**:** *W Urzędzie jest przyjęte, aby wszelkie zauważone problemy w działaniu systemów były zgłaszane do Administratora Systemów Informatycznych. I ASI, po analizie, podejmuje dalsze działania. Administrator jest pierwszą linia wsparcia, a gdy problem okaże się poważny informowane są władze Urzędu. Formalnie jest to określone w procedurze zarządzania incydentem i zapewnienia obsługi.*

W pozostałych czterech urzędach[49] nie ustanowiono procedur w zakresie zarządzania bezpieczeństwem informacji lub pomimo ustanowienia tych procedur proces ewidencjonowania incydentów był prowadzony nierzetelnie.

Szkolenia pracowników zaangażowanych w proces przetwarzania informacji

Podnoszenie świadomości zagrożeń i konsekwencji zaistnienia incydentów informacji jest istotnym elementem SZBI. Szkolenia z zakresu bezpieczeństwa informacji powinny obejmować wszystkie osoby uczestniczące w procesie przetwarzania informacji oraz dostarczać aktualnej wiedzy o nowych zagrożeniach, adekwatnych zabezpieczeniach oraz skutkach ewentualnych incydentów naruszenia bezpieczeństwa informacji. Szkolenia osób zaangażowanych w proces przetwarzania informacji powinny być prowadzone cyklicznie w związku ze zmieniającymi się zagrożeniami oraz stosowanymi zabezpieczeniami technicznymi i organizacyjnymi. Zgodnie z § 19 ust. 2 pkt 6 obowiązującego rozporządzenia KRI, szkolenie powinno uwzględniać m.in. następujące zagadnienia: zagrożenia bezpieczeństwa informacji, skutki naruszenia bezpieczeństwa informacji, w tym odpowiedzialność prawną, stosowanie środków zapewniających bezpieczeństwo informacji (np. szyfrowanie dysków, szyfrowanie kluczy USB, dostęp do systemów IT po podaniu hasła).

Stosownie do § 19 ust. 2 pkt 6 obowiązującego rozporządzenia KRI, w 14 urzędach (58 %) zorganizowano szkolenia dotyczące bezpieczeństwa informacji. Tematyka szkoleń dotyczyła m.in. zagrożeń związanych z zapewnieniem bezpieczeństwa pracy w systemach informatycznych, stosowanych środków zapewniających bezpieczeństwo informacji w urzędzie, w tym m.in.: zasad tworzenia haseł, zasad bezpiecznego użytkowania sprzętu IT, a także ochrony danych i budynków.

[49] Starostwa Powiatowe w: Ostrołęce, Sochaczewie oraz UM/UG: Osie i Otwock.

W pozostałych 10 urzędach[50] nie zapewniono szkoleń dla pracowników zaangażowanych w proces przetwarzania informacji. W odpowiedziach na wystąpienia pokontrolne, kontrolowani poinformowali o przyjęciu do realizacji wniosków NIK w ww. zakresie.

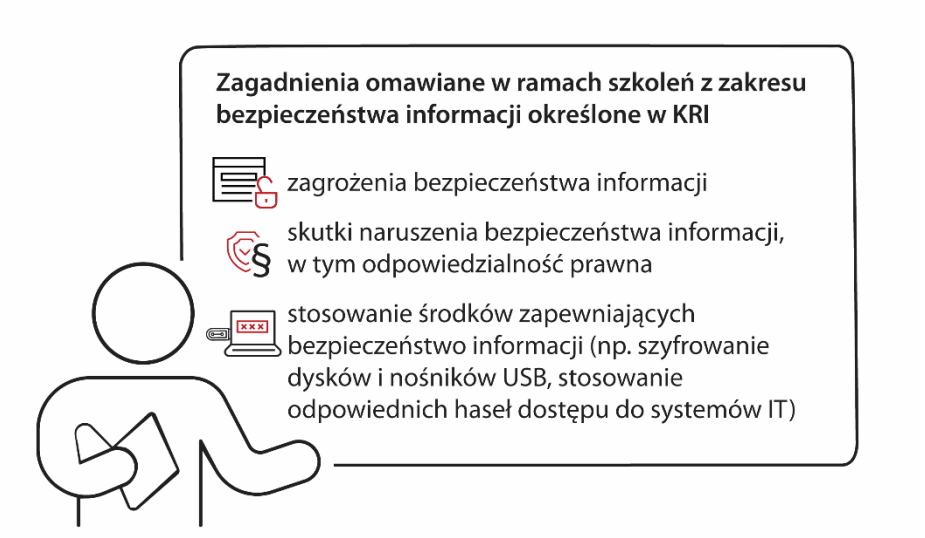
Przykład

W latach 2023–2024 w **Starostwie Powiatowym w Lubinie** nie realizowano szkoleń z zakresu bezpieczeństwa informacji.

Starosta wyjaśnił, że PBI z 2015 roku była rozpowszechniona za pośrednictwem poczty elektronicznej w trybie zwyczajowo przyjętym w starostwie, a w latach 2023–2024 nowozatrudnieni pracownicy starostwa przechodzili obowiązkowe szkolenia z ochrony danych osobowych z uwzględnieniem bezpieczeństwa informacji. Przyznał jednak, że samo oświadczenie o zapoznaniu z przepisami dotyczącymi ochrony danych osobowych nie obejmowało zapisów dotyczących zapoznania z przepisami dotyczącymi bezpieczeństwa informacji. Dodał również, że aktualna PBI rozpowszechniona została w dniu 26 czerwca 2024 r. za pośrednictwem poczty elektronicznej, a w przygotowaniu jest wersja zarządzenia wprowadzającego PBI z obowiązkiem wypełnienia oświadczenia o zapoznaniu się z treścią ww. dokumentu. Zadeklarował także, że wszyscy nowo zatrudniani pracownicy starostwa, po ukończeniu szkolenia z ochrony danych osobowych będą również szkoleni w zakresie znajomości PBI, co będzie potwierdzone podpisaniem stosownego oświadczenia.

Infografika nr 7 przedstawia zagadnienia szkoleń z zakresu bezpieczeństwa informacji wymaganych na podstawie rozporządzenia KRI.

Infografika nr 7



Źródło: opracowanie własne NIK na podstawie wyników kontroli.

[50] Starostwa Powiatowe w: Ostrołęce, Sochaczewie, Sępólnie Krajeńskim, Wąbrzeźnie, Kłodzku i Lubinie oraz UM/UG: Osie, Nowa Ruda i Świecie.

Okresowy audyt wewnętrzny z zakresu bezpieczeństwa informacji

W dziewięciu urzędach (37 %)[51] w 2023 r. nie przeprowadzono obowiązkowego audytu z zakresu bezpieczeństwa informacji, co było niezgodne z § 19 ust. 2 pkt 14 obowiązującego rozporządzenia KRI lub audyt przeprowadzono nierzetelnie, bądź z naruszeniem zasady niezależności i obiektywizmu audytu. Powyższe nieprawidłowości tłumaczono m.in. brakiem pracowników posiadających niezbędną wiedzę i doświadczenie dla przeprowadzenia takiego audytu.

Przykład

W **Urzędzie Miejskim w Nowej Rudzie**, audyt wewnętrzny z zakresu bezpieczeństwa informacji, o którym mowa w § 19 ust. 2 pkt 14 obowiązującego rozporządzenia KRI był wykonany przez pracowników Urzędu, tj. przez Inspektora Ochrony Danych oraz informatyka. W związku z faktem, że w zakresach obowiązków tych osób znajdowały się obszary dotyczące ochrony danych osobowych, czy też zarządzania systemami informatycznymi, audytowali oni obszary, za które bezpośrednio odpowiadali. Naruszało to zasady niezależności i obiektywności audytu określone w *Standardach audytu wewnętrznego dla jednostek sektora finansów publicznych*[52]. Informatyk wyjaśnił, że w związku z brakiem funduszy audyt wewnętrzny wykonano w formie samooceny, a wykonując audyt posiłkowano się szablonem audytu z lat poprzednich.

W 15 jednostkach przeprowadzono coroczny audyt bezpieczeństwa informacji. Stwierdzane w trakcie audytów problemy były zróżnicowane i dotyczyły m.in. nieokreślenia zasad i niewłaściwego dokumentowania analiz ryzyka oraz braku systemowego zarządzania uprawnieniami użytkowników, a także nieopracowania procedury zapewnienia ciągłości działania. Po przeprowadzonych audytach sformułowane zostały zalecenia-rekomendacje ukierunkowane na wzmocnienie bezpieczeństwa przetwarzania informacji.

[51] Starostwo Powiatowe w: Lubinie, Ostrołęce i Sępólnie Krajeńskim oraz UM/UG: Kamienna Góra, Kcynia, Nowa Ruda, Osie, Świecie, Świętochłowice.

[52] Komunikat Ministra Rozwoju i Finansów z dnia 12 grudnia 2016 r. w sprawie standardów audytu wewnętrznego dla jednostek sektora finansów publicznych (Dz. Urz. MRiF poz. 28).

6. ZAŁĄCZNIKI

6.1. METODYKA KONTROLI I INFORMACJE DODATKOWE

Cel główny kontroli

Czy prawidłowo, rzetelnie i skutecznie realizowano zadania związane z zapewnieniem bezpieczeństwa informacji oraz ciągłości działania systemów informatycznych w jednostkach samorządu terytorialnego?

Cele szczegółowe

1. Czy podjęto prawidłowe, rzetelne i skuteczne działania dla zapewnienia organizacji bezpieczeństwa informacji oraz dla zapewnienia ciągłości działania systemów informatycznych, tj. czy przeprowadzono odpowiednie analizy oraz czy opracowano i przyjęto do stosowania odpowiednie procedury, polityki, instrukcje oraz określono i zapewniono niezbędne zasoby osobowe i techniczne?
2. Czy prawidłowo, rzetelnie i skutecznie wdrożono przyjęte rozwiązania organizacyjne i techniczne, tj. czy są one faktycznie stosowane i egzekwowane?
3. Czy są cyklicznie podejmowane prawidłowe działania mające na celu zapobieganie incydentom bezpieczeństwa informacji (szkolenia, analiza incydentów, audyty, analiza ryzyka)?

Zakres podmiotowy

Kontrolą objęto 24 jednostki: 17 urzędów miast i gmin i siedem starostw powiatowych.

Kryteria kontroli

Kontrolę przeprowadzono na podstawie art. 2 ust. 2 ustawy o NIK z uwzględnieniem kryteriów: legalności, gospodarności i rzetelności.

Okres objęty kontrolą

Kontrolą objęto okres od 1 stycznia 2023 r. do 20 września 2024 r. Czynności kontrolne w jednostkach przeprowadzono w okresie od 23 maja 2024 r. do 20 września 2024 r.

Zgłoszono trzy zastrzeżenia do wystąpienia pokontrolnego skierowanego do Prezydenta Miasta Otwocka. Zastrzeżenia dotyczyły:

- oceny negatywnej w obszarze organizacji bezpieczeństwa informacji oraz zapewnienia ciągłości działania systemów informatycznych;
- nieprawidłowości dotyczącej nieprzeprowadzenia okresowych analiz ryzyka utraty integralności, poufności lub dostępności informacji i związanego z tą nieprawidłowością wniosku;
- nieprawidłowości dotyczącej niezidentyfikowania wszystkich posiadanych i przetwarzanych informacji; niesklasyfikowania ich z uwzględnieniem wymagań prawnych, wartości, krytyczności i wrażliwości na nieuprawnione ujawnienie lub modyfikację, nieprzypisania informacjom odpowiedniego poziomu ochrony oraz związanego z tą nieprawidłowością wniosku.

Uchwałą Komisji Rozstrzygającej NIK z dnia 13 października 2024 r. zastrzeżenia oddalono.

Stan realizacji wniosków pokontrolnych

Do kierowników jednostek kontrolowanych zostały skierowane 24 wystąpienia pokontrolne, gdzie zidentyfikowano 222 nieprawidłowości, z których 51 zostało usuniętych już w trakcie kontroli. NIK sformułowała 171 wniosków pokontrolnych. Według stanu na dzień 16 stycznia 2025 r. zrealizowano 72 wnioski, a 99 było w trakcie realizacji. Ujawnione w trakcie kontroli nieprawidłowości nie miały wymiaru finansowego.

Kierownicy kontrolowanych urzędów poinformowali NIK o podjęciu działań na rzecz realizacji wniosków pokontrolnych.

Wnioski NIK skierowane do kierowników jednostek kontrolowanych dotyczyły m.in.:

- zidentyfikowania wszystkich posiadanych i przetwarzanych zbiorów danych oraz ich sklasyfikowanie z uwzględnieniem wymagań prawnych, krytyczności i wrażliwości na modyfikację lub nieuprawnione ujawnienie,
- opracowania i wdrożenia Systemu Zarządzania Bezpieczeństwem Informacji, bądź przeglądu i aktualizacji SZBI,
- ustanowienia polityk ciągłości działania oraz opracowanie i wdrożenie planów zapewnienia ciągłości działania, planów odtworzeniowych oraz zapewnienie ich okresowego testowania,
- zapewnienia dostępu do przetwarzania informacji w zakresie adekwatnym do zadań realizowanych przez pracowników,
- zapewnienia niezwłocznego odbierania uprawnień do systemów informatycznych byłym pracownikom,
- regularnego testowania kopii zapasowych oraz przechowywanie ich poza miejscem wytworzenia,
- zapewnienia odpowiedniego poziomu zabezpieczenia fizycznego serwerowni,
- identyfikacji kluczowych elementów infrastruktury i usługi IT oraz ich zabezpieczenie pod kątem wpływu czynników zewnętrznych w związku z potrzebą zachowania ciągłości działania.

Wykaz jednostek kontrolowanych

Lp.	Jednostka organizacyjna NIK przeprowadzająca kontrolę	Nazwa jednostki kontrolowanej	Imię i nazwisko kierownika jednostki kontrolowanej
1.	Departament Administracji Publicznej	Urząd Miasta Józefowa	Marek Banaszek
		Urząd Miasta Otwocka	Jarosław Tomasz Margielski
		Urząd Miejski w Szydłowcu	Artur Ludew
		Urząd Miasta Żyrardowa	Lucjan Krzysztof Chrzanowski
		Starostwo Powiatowe w Ostrołęce	Piotr Liżewski od 7 maja 2024 r. wcześniej Stanisław Kubeł od 21 listopada 2018 r. do 6 maja 2024 r.
		Starostwo Powiatowe w Sochaczewie	Jolanta Gonta
2.	Delegatura NIK w Bydgoszczy	Urząd Miejski w Kcyni	Mateusz Stachowiak od 7 maja 2024 r. wcześniej Marek Szaruga od 20 listopada 2018 r. do 19 sierpnia 2023 r., Rafał Heftowicz od 20 sierpnia 2023 r. do 3 października 2023 r.

Lp.	Jednostka organizacyjna NIK przeprowadzająca kontrolę	Nazwa jednostki kontrolowanej	Imię i nazwisko kierownika jednostki kontrolowanej
			Wojciech Niemczyk od 4 października 2023 r. do 24 stycznia 2024 r. Rafał Heftowicz od 25 stycznia 2024 r. do 6 maja 2024 r.
		Urząd Miejski w Koronowie	Patryk Mikołajewski
		Urząd Gminy w Osiu	Michał Grabski
		Urząd Miejski w Świeciu	Krzysztof Kułakowski
		Starostwo Powiatowe w Sępólnie Krajeńskim	Jarosław Tadych
		Starostwo Powiatowe w Wąbrzeźnie	Krzysztof Maćkiewicz
3.	Delegatura NIK w Katowicach	Urząd Miejski w Czechowicach- -Dziedzicach	Marian Błachut
		Urząd Miejski w Pyskowicach	Adam Wójcik
		Urząd Miejski w Sośnicowicach	Bernard Wilczek od 6 maja 2024 r. wcześniej Leszek Kołodziej od 19 listopada 2018 r.
		Urząd Miejski w Świętochłowicach	Daniel Beger
		Urząd Gminy Zbrosławice	Katarzyna Zyga od 7 maja 2024 r. Wcześniej Wiesław Olszewski Od 19 listopada 2018 r. do 6 maja 2024 r.
		Starostwo Powiatowe w Wodzisławiu Śląskim	Leszek Bizoń
4.	Delegatura NIK we Wrocławiu	Urząd Miejski w Głogowie	Rafael Rokaszewicz
		Urząd Miasta Kamienna Góra	Janusz Chodasewicz
		Urząd Miejski w Oławie	Tomasz Frischmann
		Urząd Miejski w Nowej Rudzie	Tomasz Kiliński
		Starostwo Powiatowe w Kłodzku	Małgorzata Jędrzejewska-Skrzypczyk od 31 stycznia 2024 r. Wcześniej Maciej Awiżeń od 22 listopada 2018 r.
		Starostwo Powiatowe w Lubinie	Paweł Kleszcz

6.1.1. WYKAZ OCEN KONTROLOWANYCH JEDNOSTEK

Lp.	Nazwa jednostki kontrolowanej	Ocena kontrolowanej działalności*/	Stany mające wpływ na wydaną ocenę:	
			prawidłowe	nieprawidłowe
1.	Urząd Miasta Józefowa	w formie opisowej	• Ustanowiono i wdrożono System Zarządzania Bezpieczeństwem Informacji, a w ramach niego Politykę Bezpieczeństwa Informacji. • Powołany został Inspektor Ochrony Danych. Osoba pełniąca tę funkcję, a także inni pracownicy, którzy byli odpowiedzialni za bezpieczeństwo informacji, posiadali odpowiednie przygotowanie merytoryczne i doświadczenie zawodowe. • Wprowadzono zasady tworzenia haseł dostępu do systemów informatycznych, a zabezpieczenia komputerów pracowników uniemożliwiały zainstalowanie nieautoryzowanego oprogramowania. • Prowadzono elektroniczny rejestr zasobów teleinformatycznych, który umożliwiał weryfikację sprzętu oraz jego konfiguracji. • Wprowadzono procedurę dotyczącą zarządzania incydentami naruszenia bezpieczeństwa informacji. • Zabezpieczono serwerownię Urzędu przed nieuprawnionym dostępem. • Uprawnienia nadawano pracownikom adekwatnie do realizowanych przez nich zadań.	Stwierdzone w trakcie kontroli nieprawidłowości polegały m.in. na: • niezapewnieniu przechowywania kopii zapasowych danych z badanych systemów informatycznych poza miejscem wytwarzania danych, • nieustanowieniu polityk ciągłości działania oraz nieopracowaniu planów zapewnienia ciągłości działania oraz planów odtworzeniowych, • niedokonaniu pełnej identyfikacji aktywów informacyjnych wymagających, • niespełnieniu wymagań dla haseł dostępu użytkowników do dwóch systemów.
2.	Urząd Miasta Otwocka	w formie opisowej	• Prawidłowo realizowano zadania dotyczące opracowania spełniającej wymogi RODO dokumentacji z zakresu ochrony danych osobowych oraz gromadzenia aktualnych informacji o zasobach informatycznych obejmujących ich rodzaj i konfigurację. • Podejmowano działania zapewniające bezpieczeństwo przetwarzania informacji m.in. poprzez prawidłowe przechowywanie i testowanie kopii zapasowych, nadawanie uprawnień pracownikom adekwatnie do realizowanych przez nich zadań oraz stosowanie w umowach serwisowych postanowień gwarantujących odpowiedni poziom bezpieczeństwa informacji. • Wprowadzono procedury dotyczące przekazywania sprzętu komputerowego podmiotom zewnętrznym oraz zasady pracy zdalnej. • Podjęto działania w celu zapobiegania incydentom bezpieczeństwa informacji, tj. zorganizowano szkolenia pracowników oraz przeprowadzono audyt z tego zakresu.	• Nie ustanowiono i nie wdrożono Systemu Zarządzania Bezpieczeństwem Informacji (w szczególności Polityki Bezpieczeństwa Informacji), • Nie ustanowiono i nie wdrożono polityk w ramach zapewnienia ciągłości działania systemów informatycznych. • Stwierdzono nieprawidłowości w zakresie zapewnienia bezpieczeństwa informacji w urzędzie, które dotyczyły m.in. możliwości instalowania przez pracownika do tego nieuprawnionego nieautoryzowanego oprogramowania, niespełniania przyjętych wymagań dla haseł dostępu oraz braku blokowania kont byłych pracowników w systemach informatycznych wykorzystywanych przez urząd. • Nie prowadzono okresowych analiz ryzyka utraty integralności, poufności lub dostępności informacji, a wprowadzona w urzędzie procedura w zakresie zgłaszania incydentów naruszenia bezpieczeństwa informacji odnosiła się wyłącznie do danych osobowych.
3.	Urząd Miejski w Szydłowcu	w formie opisowej	• Ustanowiono i wdrożono System Zarządzania Bezpieczeństwem Informacji. • Ustanowiono i wdrożono Politykę Bezpieczeństwa Informacji wraz z procedurami i instrukcjami, która podlegała regularnym przeglądom. • Prawidłowo realizowano zadania w zakresie gromadzenia aktualnych informacji o zasobach informatycznych obejmujących ich rodzaj i konfigurację.	• Nie zidentyfikowano zbiorów danych (oprócz danych osobowych). • Nie ustanowiono polityki ciągłości działania, planów ciągłości działania i planów odtworzeniowych, nie przeprowadzono także analizy ryzyka w zakresie zapewnienia ciągłości działania. • Nie prowadzono okresowych analiz ryzyka utraty integralności, poufności lub dostępności informacji.

Lp.	Nazwa jednostki kontrolowanej	Ocena kontrolowanej działalności*/	Stany mające wpływ na wydaną ocenę:	
			prawidłowe	nieprawidłowe
			• Podejmowano działania zapewniające bezpieczeństwo przetwarzania informacji, m.in. poprzez testowanie kopii zapasowych, nadawanie uprawnień pracownikom adekwatnie do realizowanych przez nich zadań. • Podjęto działania w celu zapobiegania incydentom bezpieczeństwa informacji.	
4.	Urząd Miasta Żyrardowa	w formie opisowej	• Opracowano Plan ciągłości działania systemu teleinformatycznego Urzędu Miasta Żyrardowa oraz harmonogramy testów tego planu, jednak dokumenty te dotyczyły wyłącznie 2024 roku i zgodnie z nimi przeprowadzono testy. • Prezydent Miasta Żyrardowa, zgodnie z wymogami określonymi w RODO, powołał Inspektora Ochrony Danych i umożliwił mu realizację zadań w sposób niezależny. Osoba pełniąca tę funkcję, a także inni pracownicy, którzy byli odpowiedzialni za bezpieczeństwo informacji, posiadali odpowiednie przygotowanie merytoryczne i doświadczenie zawodowe. • Wprowadzono i stosowano zasady tworzenia haseł dostępu do systemów informatycznych, a zabezpieczenia komputerów pracowników uniemożliwiały zainstalowanie nieautoryzowanego oprogramowania. • Zapoznano pracowników z ustanowionymi w urzędzie zasadami pracy zdalnej i mobilnej. • Prowadzono elektroniczny rejestr zasobów teleinformatycznych, który umożliwiał weryfikację sprzętu oraz jego konfiguracji. • Objęte kontrolą umowy z podmiotami zewnętrznymi, dotyczące m.in. wsparcia oraz serwisu sprzętu informatycznego, zawierały postanowienia gwarantujące odpowiedni poziom bezpieczeństwa informacji i poufności danych. • W urzędzie wprowadzono procedury dotyczące zarządzania incydentami naruszenia bezpieczeństwa informacji, a w przypadku stwierdzenia incydentów podejmowano właściwe działania wyjaśniające i naprawcze. W urzędzie przeprowadzona została również analiza ryzyka utraty integralności, dostępności lub poufności informacji. Przeprowadzono także okresowy audyt z zakresu bezpieczeństwa informacji.	Stwierdzone w trakcie kontroli nieprawidłowości polegały m.in. na: – niesporządzeniu harmonogramów testów *Planu ciągłości działania systemu teleinformatycznego Urzędu Miasta Żyrardowa* na 2023 r. i nieprzeprowadzeniu testów tego planu w 2023 r., co było działaniem nierzetelnym i stanowiło naruszenie wytycznych określonych w punkcie 5.2. *Procedury zarządzania ciągłością działania systemu teleinformatycznego Urzędu Miasta Żyrardowa*, – niewyznaczeniu i niezgłoszeniu do CSIRT NASK, w okresie od 1 marca 2024 r. do 27 maja 2024 r., osoby odpowiedzialnej za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa, – niesporządzeniu aktualnego zakresu czynności dla jednego pracownika urzędu spośród 15 badanych, co było działaniem nierzetelnym, oraz niedokonaniu dla niego zmiany uprawnień do jednego z modułów w systemie informatycznym, – niesporządzeniu dla wszystkich 14 objętych kontrolą pracowników, którzy zakończyli pracę w urzędzie, wniosków o odebranie upoważnienia i odebranie uprawnień do korzystania z systemu informatycznego, co było działaniem nierzetelnym i stanowiło naruszenie zasad określonych w punkcie 5.5. ppkt 1 *Procedury kontroli dostępu do informacji chronionych Urzędu Miasta Żyrardowa*, – zablokowaniu dostępu do systemów informatycznych jednemu spośród 14 objętych kontrolą pracowników, którzy zakończyli pracę w urzędzie, dopiero po upływie 40 dni od rozwiązania z nim umowy o pracę.
5.	Starostwo Powiatowe w Ostrołęce	negatywna	Prawidłowo realizowano zadania w zakresie m.in.: • wyznaczenia i zapewnienia niezależności Inspektora Ochrony Danych Osobowych, • opracowania i wdrożenia dokumentacji w zakresie bezpieczeństwa danych osobowych i jej dostosowania do wymogów RODO, • wyznaczenia i zgłoszenia osób odpowiedzialnych za utrzymanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa.	W obszarze dotyczącym organizacji bezpieczeństwa informacji i zapewnienia ciągłości działania stwierdzone nieprawidłowości dotyczyły m.in.: – niezidentyfikowania wszystkich zbiorów danych urzędu podlegających zabezpieczeniu, – niewdrożenia Systemu Zarządzania Bezpieczeństwem Informacji. • Ponadto nie zostały ustanowione polityki ciągłości działania oraz plany zapewnienia ciągłości działania i plany odtworzeniowe, a, także nie prowadzono analiz ryzyka

Lp.	Nazwa jednostki kontrolowanej	Ocena kontrolowanej działalności*/	Stany mające wpływ na wydaną ocenę:	
			prawidłowe	nieprawidłowe
			Ponadto: • zapobiegano możliwości zainstalowania nieautoryzowanego oprogramowania na komputerach urzędu, • zapewniono właściwe usytuowanie komputerów w salach obsługi obywateli, aby uniemożliwić wgląd do danych przez osoby nieuprawnione, • prawidłowo wykonywano i przechowywano kopie zapasowe systemów informatycznych.	w związku z potrzebą zachowania ciągłości działania. • Nie utrzymywano także w aktualności inwentaryzacji zasobów informatycznych urzędu, rozumianej jako stałe posiadanie aktualnych informacji w zakresie posiadanego sprzętu informatycznego oraz jego konfiguracji. W obszarze rozwiązań organizacyjnych i technicznych zapewniających bezpieczeństwo informacji oraz ciągłość działania, wdrożonych i wykorzystywanych w urzędzie: – nie zapewniono adekwatności przyznawanych uprawnień przetwarzania informacji do zadań realizowanych przez pracowników, – nie ustanowiono zasad gwarantujących bezpieczną pracę przy pracy zdalnej, – nie zapewniono właściwego poziomu zabezpieczeń serwerowni urzędu, – nie zagwarantowano odpowiedniego poziomu bezpieczeństwa informacji w umowach w sprawie usług IT, – nie zidentyfikowano kluczowych elementów infrastruktury i usług IT pod kątem wpływu czynników zewnętrznych. W zakresie działań w celu zapobiegania incydentom bezpieczeństwa, nieprawidłowości dotyczyły m.in.: – nieprzeprowadzania okresowych audytów bezpieczeństwa, – nieopracowania procedur umożliwiających bezzwłoczne zgłaszanie incydentów naruszenia bezpieczeństwa informacji oraz incydentów cyberbezpieczeństwa, – niezapewnienia pracownikom szkoleń z zakresu bezpieczeństwa informacji i cyberbezpieczeństwa.
6.	Starostwo Powiatowe w Sochaczewie	negatywna	• Prawidłowo realizowano zadania dotyczące m.in.: opracowania dokumentacji w zakresie bezpieczeństwa przetwarzania danych osobowych i jej dostosowania do wymogów RODO, zidentyfikowania zbiorów danych w tym danych osobowych podlegających zabezpieczeniu, zabezpieczenia komputerów przed możliwością instalowania dowolnego oprogramowania przez użytkowników, a także w zakresie monitorowania zajętości dysków.	W szczególności w Urzędzie: • nie opracowano i nie wdrożono Systemu Zarządzania Bezpieczeństwem Informacji; • nie dokonywano przeglądów Polityki Bezpieczeństwa Informacji w zakresie dotyczącym zmieniającego się otoczenia; • nie podjęto wystarczających działań w związku z zapewnieniem ciągłości działania (m.in.: nie prowadzano analizy ryzyka w tym zakresie, a także nie wdrożono odpowiednich polityk i procedur); • nie prowadzono pełnej inwentaryzacji zasobów informatycznych obejmujących ich rodzaj i konfigurację; • dodatkowe zadania i obowiązki wykonywane przez osobę będącą zastępcą Inspektora Ochrony Danych powodowały konflikt interesów z zadaniami IOD; • nie testowano kopii zapasowych i w niewłaściwy sposób je przechowywano. Ustanowione

Lp.	Nazwa jednostki kontrolowanej	Ocena kontrolowanej działalności*/	Stany mające wpływ na wydaną ocenę:	
			prawidłowe	nieprawidłowe
				w Polityce Bezpieczeństwa Informacji procedury w tym zakresie nie były przestrzegane. Kopie zapasowe były przechowywane w miejscu wytwarzania danych, co w przypadku zdarzenia losowego (np. pożar) doprowadziłoby do utraty zarówno danych, jak i ich kopii; • nie zapewniono pracownikom szkoleń z zakresu bezpieczeństwa informacji; • nie prowadzono okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji, a także nie wdrożono kompleksowej procedury bezzwłocznego zgłaszania incydentów naruszenia bezpieczeństwa informacji.
7.	Urząd Miejski w Kcyni	w formie opisowej	• Urząd podjął działania dla zapewnienia bezpieczeństwa informacji, w tym opracowano Politykę Bezpieczeństwa Informacji oraz powołano niezależnego Inspektora Ochrony Danych. Nadawano uprawnienia pracownikom adekwatnie do realizowanych przez nich zadań. Wprowadzono również procedury dotyczące przekazywania sprzętu komputerowego podmiotom zewnętrznym oraz zasady pracy zdalnej. • Podjęto działania w celu zapobiegania incydentom bezpieczeństwa informacji, tj. zorganizowano szkolenia pracowników oraz dokonano analizy zagrożeń i ryzyka przy przetwarzaniu danych osobowych, w tym poufności, integralności i rozliczalności systemów informatycznych.	• Nie przeprowadzano w okresie objętym kontrolą testów sprawdzających odtworzenie systemu, aplikacji, bazy danych lub dokumentów z kopii, a także nie utrzymywano aktualności inwentaryzacji sprzętu służącego do przetwarzania informacji. Ponadto nie ustanowiono polityk ciągłości działania i nie opracowano planów zapewnienia ciągłości działania oraz planów odtworzeniowych. • Nie zapewniono odpowiednich warunków przechowywania kopii zapasowych danych oraz nie zabezpieczono informacji w sposób uniemożliwiający nieuprawnionemu ujawnienie, modyfikację, usunięcie lub zniszczenie. • Nie przeprowadzano testowego sprawdzenia odtworzenia systemu, aplikacji, bazy danych lub dokumentów z kopii. • Spośród 10 pracowników urzędu posiadających uprawnienia użytkownika, których stosunek pracy ustał, konta trzech nie zostały zablokowane. • Nie przeprowadzono audytu wewnętrznego z zakresu bezpieczeństwa informacji. • Nie prowadzono rejestru incydentów zgodnie z przyjętą procedurą i nie dołożono wystarczającej staranności w realizacji działań naprawczych.
8.	Urząd Miejski w Koronowie	w formie opisowej	• W urzędzie prawidłowo opracowano i wdrożono System Zarządzania Bezpieczeństwem Informacji. Właściwie zidentyfikowano wszystkie zbiory danych urzędu podlegające zabezpieczeniu oraz prowadzono pełną inwentaryzację zasobów informatycznych obejmującą ich rodzaj i konfigurację. Inspektorowi Ochrony Danych umożliwiono wykonywanie obowiązków w sposób niezależny. Prawidłowo w okresie objętym kontrolą, szacowano ryzyka w zakresie bezpieczeństwa teleinformatycznego. Zabezpieczenia techniczne systemów informatycznych, przyjęte w Urzędzie zapewniały ochronę przetwarzanych informacji przed nieuprawnionym dostępem. Pomieszczenie serwerowni posiadało odpowiednie zabezpieczenia. Prawidłowo tworzono i przechowywano	• Za nieprawidłowe uznano: – nieopracowanie planu odtworzeniowego oraz nieokreślenie akceptowalnego czasu przywrócenia ciągłości działania systemów informatycznych, – nieprzestrzeganie Procedury kontroli dostępu do informacji obowiązującej w urzędzie w zakresie likwidacji kont użytkowników, – brak procedur monitorowania pojemności pamięci masowych (dysków twardych) istotnych z punktu widzenia zachowania ciągłości działania serwerów.

Lp.	Nazwa jednostki kontrolowanej	Ocena kontrolowanej działalności*/	Stany mające wpływ na wydaną ocenę:	
			prawidłowe	nieprawidłowe
			kopie zapasowe zbiorów danych, programów i oprogramowania systemowego zapewniające ciągłość działania systemu informatycznego. Prawidłowo opracowano i wdrożono zasady bezpiecznego korzystania z informatycznego sprzętu mobilnego przy pracy zdalnej. Podejmowano prawidłowe działania w celu zapobiegania incydentom bezpieczeństwa informacji.	
9.	Urząd Gminy w Osiu	w formie opisowej	• W okresie objętym kontrolą urząd podejmował działania na rzecz zapewnienia bezpieczeństwa informacji, w tym danych osobowych, systemów teleinformatycznych oraz ciągłości działania. • Jednostka zidentyfikowała zbiory zawierające dane osobowe oraz wskazała programy zastosowane do ich przetwarzania. Przygotowano ponadto kluczowe regulacje wewnętrzne tworzące systemu zarządzania bezpieczeństwem informacji w jednostce. • W urzędzie wyznaczono osoby odpowiedzialne za bezpieczeństwo informacji, w tym Inspektora Ochrony Danych, któremu zapewniono niezależność. IOD, od 28 lutego 2023 r., miał także możliwość działania bez ryzyka wystąpienia konfliktu interesów. Brak było zapewnienia przez urząd takiej możliwości przed ww. terminem. • Jednostka wykonywała także działania mające na celu ochronę zasobów informacyjnych. • W jednostce podejmowano kroki w celu zapobiegania incydentom bezpieczeństwa informacji, szczególnie w zakresie analizy ryzyka utraty atrybutów bezpieczeństwa.	• Nie prowadzono, poza Polityką bezpieczeństwa danych osobowych, przeglądu oraz aktualizacji przyjętych procedur i regulaminów. • Zidentyfikowano nieprawidłowości w realizacji przyjętych procedur i obowiązków, w tym naruszających regulacje rozporządzenia KRI. Stwierdzono m.in. niezachowanie zasad dotyczących możliwości instalowania nieautoryzowanego oprogramowania, tworzenia i weryfikacji haseł, szyfrowania laptopów, przygotowania serwerowni oraz tworzenia, przechowywania i testowania kopii zapasowych, a także monitowania pojemności nośników pamięci serwerów. • W 2023 r. nie przeprowadzono jednak audytu bezpieczeństwa informacji, a proces ewidencji incydentów związanych z bezpieczeństwem informacji był prowadzony w sposób nierzetelny.
10.	Urząd Miejski w Świeciu	w formie opisowej	• W kontrolowanym okresie w urzędzie podejmowano działania na rzecz zapewnienia bezpieczeństwa informacji. Opracowano i wdrożono System Zarządzania Bezpieczeństwem Informacji oraz zapewniono aktualność dokumentów i polityk wchodzących w jego skład. Inspektorowi Ochrony Danych umożliwiono wykonywanie obowiązków w sposób niezależny. • W celu ochrony systemów informatycznych przed nieuprawnionym dostępem, określono i stosowano zasady bezpieczeństwa oraz politykę haseł. • Pracownicy uczestniczyli w procesie przetwarzania informacji w stopniu adekwatnym do realizowanych przez nich zadań, zaś po zakończeniu zatrudnienia blokowano im dostęp do systemów informatycznych. • Wprowadzono środki organizacyjne, fizyczne i techniczne zapewniające bezpieczeństwo informacji znajdujących się na serwerach. • W ramach zapewnienia ciągłości działania urzędu ustalono i stosowano zasady tworzenia i przechowywania kopii zapasowych.	• Nie dokumentowano prowadzonych analiz ryzyka utraty integralności, dostępności lub poufności informacji, a pracownikom zaangażowanym w proces przetwarzania informacji nie zapewniono szkoleń zakresu cyberbezpieczeństwa. • Audyt wewnętrzny w zakresie bezpieczeństwa informacji, z uwagi na powierzenie jego realizacji pracownikom odpowiadającym za przedmiot audytu, pozbawiony został przymiotu niezależności i obiektywizmu. • Burmistrz nie powołał pełnomocnika do spraw bezpieczeństwa informacji, choć zobowiązał się do tego wydając zarządzenie, a zgłoszenia osoby odpowiedzialnej za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa dokonano z naruszeniem ustawowego terminu. • Przyjęte w urzędzie plany zapewnienia ciągłości działania oraz plany odtworzeniowe nie były testowane, przez co ich praktycznej skuteczności nie można było zweryfikować. • W urzędzie nie przeprowadzano regularnych testów tworzonych kopii zapasowych danych i oprogramowania.

Lp.	Nazwa jednostki kontrolowanej	Ocena kontrolowanej działalności*/	Stany mające wpływ na wydaną ocenę:	
			prawidłowe	nieprawidłowe
			• Opracowano także procedurę zgłaszania i postępowania z incydentami naruszenia bezpieczeństwa informacji.	• Nie zidentyfikowano też kluczowych elementów infrastruktury i usług IT oraz ich zabezpieczeń pod kątem wpływu czynników zewnętrznych.
11.	Starostwo Powiatowe w Sępólnie Krajeńskim	w formie opisowej	• W kontrolowanym okresie w starostwie podejmowano działania na rzecz zapewnienia bezpieczeństwa informacji i ciągłości działania. Skoncentrowano je jednak wokół ochony danych osobowych. W starostwie obowiązywała Polityka Bezpieczeństwa Przetwarzania Danych Osobowych odwołująca się do szeregu procedur wewnętrznych, w szczególności dotyczących zarządzania systemem informatycznym. Odniesiono się w nich do najważniejszych zagadnień związanych z bezpieczeństwem informacji takich jak: zarządzanie uprawnieniami, uwierzytelnianie dostępu, tworzenie kopii zapasowych, przygotowanie sprzętu do wydania na zewnątrz. • Posiadano również ocenę ryzyka dla utraty atrybutów bezpieczeństwa informacji, a jednocześnie naruszenia praw i wolności osób fizycznych, z opisem stosowanych w starostwie środków obniżających jego poziom. Istotną słabością przyjętych rozwiązań było jednakże nieobjęcie nimi informacji spoza katalogu danych osobowych. Wynikało to z niepełnej identyfikacji zasobów informacyjnych podlegających ochronie. Ponadto niektóre procedury, w szczególności dotyczące zarządzania uprawnieniami i kopiami zapasowymi oraz plan ciągłości działania były nieprecyzyjne. • W starostwie wyznaczono osoby odpowiedzialne za bezpieczeństwo informacji, w tym Inspektora Ochrony Danych, któremu zapewniono niezależność i możliwość działania w sytuacji braku konfliktu interesów.	Stwierdzone nieprawidłowości dotyczyły w szczególności: – stosowania przez dwóch pracowników haseł dostępu do systemu informatycznego nieodpowiadającego wymogom PBPDO; – nadaniu jednemu użytkownikowi (z 13 analizowanych) nadmiernych uprawnień w systemie operacyjnym komputera; – opóźnień w odbieraniu uprawnień do pracy w systemach teleinformatycznych; – naruszenia przepisów wewnętrznych przy przechowywaniu kopii zapasowych; – nieustanowienia zasad gwarantujących bezpieczną pracę na odległość; – niewdrożenia środków technicznych i organizacyjnych minimalizujących ryzyko wskazanych jako rozwiązania stosowane w dokumencie *Ocena ryzyka naruszenia praw i wolności osób fizycznych;* – nie zawarcia w dwóch umowach utrzymania oprogramowania zapisów zobowiązujących wykonawcę do zachowania w tajemnicy informacji, do jakich może mieć dostęp w ramach wykonywania umowy, innych niż dane osobowe.
12.	Starostwo Powiatowe w Wąbrzeźnie	w formie opisowej	• W urzędzie prawidłowo opracowano i wdrożono system zarządzania bezpieczeństwem informacji, jednak nie dokonywano przeglądów i aktualizacji dokumentów i polityk wchodzących w jego skład, co oceniono negatywnie. • Właściwie zidentyfikowano wszystkie zbiory danych urzędu podlegające zabezpieczeniu oraz prowadzono pełną inwentaryzację zasobów informatycznych. Umożliwiono Inspektorowi Ochrony Danych wykonywanie obowiązków w sposób niezależny. • Pozytywnie oceniono przeprowadzanie, w okresie objętym kontrolą, szacowania ryzyka w zakresie bezpieczeństwa teleinformatycznego. • Zabezpieczenia techniczne systemów informatycznych, przyjęte w starostwie zapewniały ochronę przetwarzanych informacji przed nieuprawnionym dostępem. • Ustawienie monitorów objętych badaniem zapewniało, że dane wyświetlane na ekranie nie były widoczne dla osób nieuprawnionych.	Nieprawidłowości stwierdzone w toku kontroli dotyczyły: – nieprzestrzegania procedury nadawania/zmiany uprawnień do systemów informatycznych; – nieopracowania planu odtworzeniowego oraz nieokreślenia akceptowalnego czasu przywrócenia ciągłości działania systemów informatycznych; – nieprzeprowadzenia audytu wewnętrznego z zakresu bezpieczeństwa informacji; – niezawierania w umowach z podmiotami zewnętrznymi zapisów zobowiązujących wykonawców do zachowania poufności. Jako działania nieprawidłowe uznano również niezapewnianie szkoleń pracownikom starostwa zaangażowanych w proces przetwarzania informacji.

Lp.	Nazwa jednostki kontrolowanej	Ocena kontrolowanej działalności*/	Stany mające wpływ na wydaną ocenę:	
			prawidłowe	nieprawidłowe
			• Prawidłowo opracowano zasady bezpiecznego korzystania z informatycznego sprzętu mobilnego oraz dokonywano na nim szyfrowania danych. • Zarządzano pojemnością serwerów w sposób gwarantujący wydajność systemów a pomieszczenie serwerowni posiadało odpowiednie zabezpieczenia. • Należycie tworzono i przechowywano kopie zapasowe zbiorów danych, programów i oprogramowania systemowego zapewniające ciągłość działania systemu informatycznego, jednak nie były one regularnie testowane, co uznano jako nieprawidłowe. • Urząd przeprowadził analizę ryzyka utraty integralności, dostępności lub poufności informacji oraz podjął działania adekwatnie do jej wyników. Opracowana procedura zgłaszania incydentów naruszenia bezpieczeństwa informacji została przedstawiona do zapoznania się i stosowania pracownikom urzędu.	
13.	Urząd Miejski w Czechowicach--Dziedzicach	w formie opisowej	• Opracowano i wdrożono System Zarządzania Bezpieczeństwem Informacji jak i prawidłowo realizowano zadania dotyczące m.in.: opracowania dokumentacji w zakresie bezpieczeństwa przetwarzania danych osobowych i jej dostosowania do wymogów RODO. • W Polityce Bezpieczeństwa Informacji urzędu i jej aktualizacji zostały zidentyfikowane zbiory danych podlegające zabezpieczeniu, jednakże nie przypisano im odpowiedniego poziomu ochrony oraz nie określono do nich wag. • W urzędzie wyznaczono Zespół ds. bezpieczeństwa informacji. • W okresie kontrolowanym urząd dokonał przeglądu PBI. • W urzędzie wdrożono i wykorzystywano rozwiązania organizacyjne i techniczne, w tym m.in. w zakresie polityki haseł, jak i zabezpieczenia komputerów służbowych przed zainstalowaniem na nich nieautoryzowanego oprogramowania, komputery na stanowiskach pracy w miejscach obsługi obywateli zabezpieczone były przed wglądem osób nieuprawnionych, a pracownicy merytoryczni mieli dostęp do oprogramowania zgodnie z rejestrem prowadzonym przez Wydział Informatyki. • Podjęto działania w celu zapobiegania incydentom bezpieczeństwa informacji tj. przeprowadzono okresowe analizy ryzyka utraty integralności, poufności lub dostępności informacji. • W jednostce przeprowadzono okresowy audyt wewnętrzny w zakresie bezpieczeństwa informacji.	• Plan ochrony i zapewnienia ciągłości działania urzędu nie był kompletny, gdyż nie zawierał: procedur: typologii sieci, systemowych serwerów wirtualnych oraz urządzeń brzegowych, jak i procedury czasu przywrócenia ciągłości działania, jak i nie podlegał testowaniu i treningowi. • Urząd nie zidentyfikował kluczowych elementów infrastruktury i usług IT. • W serwerowni pomieszczeniu podlegającemu szczególnej ochronie znajdowały się materiały łatwopalne.

Lp.	Nazwa jednostki kontrolowanej	Ocena kontrolowanej działalności*/	Stany mające wpływ na wydaną ocenę:	
			prawidłowe	nieprawidłowe
14.	Urząd Miejski w Pyskowicach	w formie opisowej	• Urząd, prawidłowo, rzetelnie wdrożył przyjęte rozwiązania organizacyjne w zakresie ochrony bezpieczeństwa informacji. Dostęp do pomieszczeń i systemów informatycznych był ograniczany jedynie do osób upoważnionych, a pomieszczenia serwerowni oraz systemy informatyczne miały wdrożone zabezpieczenia. Zidentyfikowano również kluczowe i podlegające ochronie elementy infrastruktury informatycznej. Testowano scenariusze postępowania w przypadku awarii infrastruktury teletechnicznej, jak i przywracanie danych z kopii zapasowych. • Prowadzone były również analizy ryzyka w zakresie zapewnienia ciągłości działania oraz przeprowadzono audyty w zakresie bezpieczeństwa informacji, prowadzono rejestr incydentów oraz dokumentację z tym związaną. • Pracownicy urzędu byli przeszkoleni w zakresie zapewnienia bezpieczeństwa informacji. • Terminowo zostały wyznaczone i zgłoszone osoby odpowiedzialne za utrzymanie kontaktów z podmiotami Krajowego Systemu Cyberbezpieczeństwa, a powołany Inspektor Ochrony Danych Osobowych, któremu zagwarantowano niezależność, posiadał niezbędne kwalifikacje do wykonywania swych zadań. W działalności IOD nie zachodził również konflikt interesów.	• Niezastosowanie się w pełni do zapisów przyjętej procedury w zakresie kopii zapasowych, co skutkowało brakiem sporządzania kopii zapasowych na dodatkowych zewnętrznych nośnikach takich jak: taśmy magnetyczne, płyty CD lub DVD.
15.	Urząd Miejski w Sośnicowicach	w formie opisowej	• Wdrożono rozwiązania organizacyjne i techniczne w zakresie bezpieczeństwa informacji takich jak stosowanie haseł dostępu do systemów informatycznych, zapobieganie utracie informacji lub nieuprawnionemu dostępowi w związku z realizacją procedur serwisowych, zarządzanie pojemnością wykorzystywanych systemów informatycznych w sposób dający zapewnienie właściwej wydajności systemów, stosowanie zabezpieczeń przed szkodliwym oprogramowaniem, zidentyfikowanie kluczowych elementów infrastruktury IT, ustanowienie zasad (procedur) bezpiecznej pracy zdalnej, w tym przy przetwarzaniu mobilnym i pracy na odległość.	• Nie przypisano zbiorom danych urzędu podlegających zabezpieczeniu odpowiedniego poziomu ochrony, • Nie funkcjonował System Zarządzania Bezpieczeństwem Informacji, nie aktualizowano kart ryzyka w Analizie ryzyka w celu oceny skuteczności zastosowanych działań minimalizujących ryzyka, • Nie podjęto żadnych działań w związku z zapewnieniem ciągłości działania urzędu, • Występował konflikt interesów przy realizacji audytu bezpieczeństwa informacji, • Nie prowadzono okresowych analiz ryzyka utraty integralności, poufności lub dostępności informacji.
16.	Urząd Miejski w Świętochłowicach	w formie opisowej	W latach 2023–2024 urząd podejmował działania mające na celu zapewnienie bezpieczeństwa informacji oraz ciągłości działania systemów informatycznych. Podejmowane działania polegały m.in. na: • opracowaniu Polityki Bezpieczeństwa Urzędu Miasta dotyczącej bezpieczeństwa danych osobowych jednakże zawierającej również elementy związane z zasobami informatycznymi Urzędu i ich zabezpieczeniem;	• W urzędzie nie ustanowiono i wdrożono SZBI. • Nierzetelne działanie jednostki kontrolowanej dotyczyło nieprzypisania zbiorom danych kategorii ochrony, nieopracowania polityki ciągłości działania oraz planów ciągłości działania i planów odtworzeniowych. Z uwagi na nieopracowanie ww. planów nie wyznaczono również osób odpowiedzialnych za ciągłość działania systemów informatycznych Urzędu.

Lp.	Nazwa jednostki kontrolowanej	Ocena kontrolowanej działalności*/	Stany mające wpływ na wydaną ocenę:	
			prawidłowe	nieprawidłowe
			• przeprowadzaniu analiz ryzyka w zakresie zapewnienia ciągłości działania; • przeprowadzaniu corocznych audytów z zakresu bezpieczeństwa informacji; • opracowaniu procedur i instrukcji stanowiących dokumenty wykonawcze do Polityki bezpieczeństwa; • opracowaniu regulaminu pracy wykonywanej w formie zdalnej. • Urząd posiadał pełną informację o posiadanych zasobach informatycznych oraz o zbiorach przetwarzanych danych podlegających zabezpieczeniu i ochronie. • Pracownicy uzyskiwali adekwatne do realizowanych zadań dostępy do rejestrów, baz danych, systemów dziedzinowych, a konta pracowników, którzy zakończyli pracę były zamykane w momencie powzięcia przez pracowników Wydziału Informatyki informacji o odejściu pracownika. • Służbowy sprzęt IT został zabezpieczony przed dostępem osób nieuprawnionych oraz zainstalowaniem nieautoryzowanego oprogramowania. Na służbowych telefonach komórkowych użytkownicy mogli instalować oprogramowanie z zewnątrz. • Serwerownia i miejsce przechowywania kopii zapasowych zostały prawidłowo zabezpieczone przed dostępem osób nieuprawnionych. Kopie zapasowe były tworzone i testowane na bieżąco, a sposób ich utworzenia umożliwiał odzyskanie zapisanych danych. • Pracownicy urzędu zostali przeszkoleni z zakresu Cyberbezpieczeństwa i zapoznani z zasadami zapewnienia bezpieczeństwa informacji.	
17.	Urząd Gminy Zbrosławice	w formie opisowej	• Przyjęto i wdrożono system zarządzania bezpieczeństwem informacji wraz z dokumentami składającymi się na ten system, w tym politykę bezpieczeństwa informacji, instrukcję zarządzania systemem informatycznym, plan ciągłości działania oraz zasady pracy zdalnej. • Zidentyfikowano kluczowe elementy infrastruktury IT oraz nadano im poziom wrażliwości. • Powołanemu Inspektorowi Ochrony Danych Osobowych zagwarantowano niezależne wykonywanie obowiązków. • Administratorowi Systemów Informatycznych przypisano odpowiedzialność za zapewnienie bezpieczeństwa informacji oraz ciągłości działania. • Wyznaczono osobę do utrzymywania kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa. • Pracowników urzędu zapoznano z procedurami składającymi się na system zarządzania bezpieczeństwem informacji, zapewniono im także szkolenia z zakresu ochrony danych osobowych oraz szkolenie z zakresu cyberbezpieczeństwa.	Stwierdzone w toku kontroli nieprawidłowości dotyczyły m.in.: – niedokonania bezzwłocznego blokowania dostępu do systemów informatycznych ośmiu spośród 15 objętych badaniem pracowników, którzy zakończyli pracę w urzędzie, – przechowywania kopii zapasowych w miejscu wytwarzania danych, – wbrew regulacjom wewnętrznym zrezygnowano z wymuszenia okresowej zmiany haseł w odniesieniu do dwóch z trzech objętych badaniem programów komputerowych, – wprowadzono istotne dla systemu bezpieczeństwa informacje, po przeszło 300dniach od otrzymania rekomendacji audytora: wykazu systemów informatycznych z określonym poziomem krytyczności, wykazu usług i elementów infrastruktury istotnej z punktu widzenia zachowania ciągłości działania, procedur dotyczących kopii zapasowych obejmujących m.in. ich przechowywanie i częstotliwość ich sporządzania, regulacji wewnętrznych związanych z systemem dostępu do pomieszczeń urzędu.

Lp.	Nazwa jednostki kontrolowanej	Ocena kontrolowanej działalności*/	Stany mające wpływ na wydaną ocenę:	
			prawidłowe	nieprawidłowe
			• Przeprowadzono audyt z zakresu bezpieczeństwa informacji. • Pracownikom uniemożliwiono instalację na komputerach dowolnego oprogramowania. • Usytuowanie monitorów na stanowiskach pracy uniemożliwiało wgląd do danych przez osoby nieuprawnione. • Pomieszczenie serwerowni było zabezpieczone w sposób ograniczający ryzyko nieuprawnionego dostępu z zewnątrz. • W umowach na serwis i dostawę urządzeń ujmowano zapisy dotyczące zachowania poufności informacji uzyskanych w związku z realizacją umów. • Przeprowadzono, w okresie objętym kontrolą, kilkukrotne testowanie odtwarzania kopii zapasowych.	
18.	Starostwo Powiatowe w Wodzisławiu Śląskim	w formie opisowej	• W starostwie prawidłowo opracowano i wdrożono procedury mające na celu zapewnienie bezpieczeństwa informacji oraz ciągłości działania systemów informatycznych, procedury te były aktualizowane. Zapewniono również odpowiednie zasoby kadrowe dla zachowania bezpieczeństwa informacji i ciągłości działania z jednoczesnym przypisaniem obowiązków /odpowiedzialności w tym zakresie. • Starostwo, prawidłowo wdrożyło przyjęte rozwiązania organizacyjne w zakresie ochrony bezpieczeństwa informacji. • Wykorzystywane w starostwie systemy informatyczne oraz osprzęt informatyczny były zabezpieczane hasłami dostęp; pomieszczenia krytycznej infrastruktury informatycznej (serwerownie) były zabezpieczone przed dostępem osób postronnych, serwery starostwa były zabezpieczone przed nagłą utratą zasilania w urządzenia podtrzymujące zasilanie. • Znajdujące się na wyposażeniu starostwa komputery były chronione oprogramowaniem obejmującym m.in. ochronę systemu plików, system zapobiegania włamaniom (IPS), ochronę przed atakami z sieci (IDS), firewall, ochronę dostępu do stron internetowych i poczty e-mail. • Dostęp do pomieszczeń i systemów informatycznych został ograniczony do osób upoważnionych; w jednej z serwerowni starostwa nie dokonywano wymaganych procedurami wpisów o osobach niebędących pracownikami starostwa, które przebywały w serwerowni pod nadzorem upoważnionego pracownika. • Pomieszczenia serwerowni oraz narzędzia informatyczne, w tym systemy informatyczne zostały zabezpieczone kontrolą dostępu. W dwóch poddanych oględzinom pomieszczeniach serwerowni znajdowały się materiały łatwopalne, które mogły zwiększyć ryzyko utraty danych w przypadku ewentualnego pożaru.	• W jednej z serwerowni starostwa w ewidencji wejść/wyjść nie odnotowywano przebywania osób niebędących pracownikami Biura Informatyki, co było niezgodne z pkt 4, część 3 *procedury Zabezpieczenia fizyczne* dział *Dostęp do serwerowni.* • W dwóch serwerowniach starostwa znajdowały się materiały łatwopalne – kartony.

Lp.	Nazwa jednostki kontrolowanej	Ocena kontrolowanej działalności*/	Stany mające wpływ na wydaną ocenę:	
			prawidłowe	nieprawidłowe
			• W starostwie zapewniono bezpieczeństwo danych m.in. poprzez sporządzanie i przechowywanie kopii zapasowych, które były poddawane testowaniu oraz identyfikację kluczowych elementów infrastruktury informatycznej. • W jednostce prowadzono również analizy ryzyka w zakresie zapewnienia ciągłości działania oraz przeprowadzono stosowne audyty. • Pracownicy starostwa byli przeszkoleni w zakresie zapewnienia bezpieczeństwa informacji. Starostwo prowadziło również rejestr incydentów oraz dokumentację z tym związaną.	
19.	Urząd Miejski w Głogowie	pozytywna	• W badanym okresie stosowano dokumentację składającą się na System Zarządzania Bezpieczeństwem Informacji i Politykę Ochrony Danych Osobowych, uwzględniającą wymogi odpowiednio rozporządzenia KRI oraz RODO. • Przeprowadzono także przegląd SZBI oraz okresowy audyt wewnętrzny z zakresu bezpieczeństwa informacji. • Ponadto w urzędzie prawidłowo zidentyfikowano zbiory danych podlegających zabezpieczeniu oraz kluczowe elementy infrastruktury i usług IT. • Prowadzono także niezbędne analizy ryzyka oraz sporządzono odpowiednią dokumentację w celu m.in. zapewnienia ciągłości działania, określenia bezpiecznych zasad pracy zdalnej, określenia zasad tworzenia i przechowywania kopii zapasowych, nadawania i odbierania pracownikom uprawnień do pracy w systemach informatycznych oraz postępowania w sytuacjach wystąpienia lub podejrzenia wystąpienia incydentu w zakresie bezpieczeństwa informacji. • Prawidłowo określono i zapewniono także niezbędne zasoby osobowe i techniczne w celu zapewnienia bezpieczeństwa informacji oraz przeprowadzano szkolenia pracowników odpowiedzialnych za przetwarzanie informacji. • Wdrożono również właściwie rozwiązania organizacyjne i techniczne zapobiegające możliwości instalowania nieautoryzowanego oprogramowania, zabezpieczono pomieszczenie serwerowni, a także regularnie tworzono i testowano kopie zapasowe danych.	• Nie stwierdzono nieprawidłowości.
20.	Urząd Miasta Kamienna Góra	w formie opisowej	• Urząd nie zawsze prawidłowo i rzetelnie realizował zadania związane z zapewnieniem bezpieczeństwa informacji oraz ciągłości działania systemów informatycznych. • W okresie objętym kontrolą stosowano dokumentację składającą się na System Zarządzania Bezpieczeństwem Informacji i Politykę Ochrony Danych, uwzględniającą wymogi odpowiednio rozporządzenia KRI oraz RODO.	• Stwierdzono nieprawidłowości polegające na: – nierzetelnym sporządzeniu dokumentacji związanej z zapewnieniem ciągłości działania systemów informatycznych, – nadmiarowym udostępnieniu wszystkim pracownikom urzędu szczegółowych zasad zarządzania środowiskiem informatycznym, – nie w pełni rzetelnej aktualizacji SZBI,

Lp.	Nazwa jednostki kontrolowanej	Ocena kontrolowanej działalności*/	Stany mające wpływ na wydaną ocenę:	
			prawidłowe	nieprawidłowe
			• Ponadto w urzędzie prawidłowo zidentyfikowano zbiory danych podlegających zabezpieczeniu oraz kluczowe elementy infrastruktury i usług IT. • Prowadzono także niezbędne analizy ryzyka oraz sporządzono odpowiednią dokumentację w celu m.in. zapewnienia ciągłości działania, określenia zasad tworzenia i przechowywania kopii zapasowych, nadawania i odbierania pracownikom uprawnień do pracy w systemach informatycznych oraz postępowania w sytuacjach wystąpienia lub podejrzenia wystąpienia incydentu w zakresie bezpieczeństwa informacji. • Prawidłowo określono i zapewniono także niezbędne zasoby osobowe i techniczne w celu zapewnienia bezpieczeństwa informacji oraz przeprowadzano szkolenia pracowników odpowiedzialnych za przetwarzanie informacji. • Wdrożono również właściwie rozwiązania organizacyjne i techniczne zapobiegające możliwości instalowania nieautoryzowanego oprogramowania, zabezpieczono pomieszczenie serwerowni systemami przeciwwłamaniowymi oraz przeciwpożarowymi, a także regularnie tworzono i testowano kopie zapasowe danych.	– niesporządzeniu wewnętrznych regulacji dotyczących pracy zdalnej, przewidzianych w SZBI, – użytkowania pomieszczenia serwerowni w sposób niezapewniający odpowiedniej ochrony przeciwpożarowej, – nieprawidłowym przechowywaniu nośników danych z kopiami zapasowymi, – udzieleniu pracownikom dostępu do systemów informatycznych bez stosownego upoważnienia lub ze zbyt ogólnym upoważnieniem, – niezablokowaniu kont w systemach IT byłym pracownikom urzędu, – ustaleniu wymogów dla haseł w jednym z systemów informatycznych niezgodnie z wymogami SZBI, – braku w dwóch umowach serwisowych zapisów gwarantujących odpowiedni poziom bezpieczeństwa informacji, – nieprzeprowadzeniu w 2023 r. okresowego, corocznego audytu wewnętrznego z zakresu bezpieczeństwa informacji.
21.	Urząd Miejski w Oławie	w formie opisowej	• Urząd nie zawsze prawidłowo i rzetelnie realizował zadania związane z zapewnieniem bezpieczeństwa informacji oraz ciągłości działania systemów informatycznych. • W okresie objętym kontrolą opracowano i wdrożono System Zarządzania Bezpieczeństwem Informacji. • Sporządzono także dokumentację w zakresie ochrony danych osobowych uwzględniającą wymogi RODO. • Prawidłowo zidentyfikowano również zbiory danych podlegających zabezpieczeniu. • Wyznaczono pracowników odpowiedzialnych za bezpieczeństwo informacji, zapewnienie ciągłości działania, ochronę danych osobowych oraz za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa. • Utrzymywano aktualność inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji obejmującej ich rodzaj i konfigurację. • Wprowadzono rozwiązania zapobiegające możliwości instalowania nieautoryzowanego oprogramowania, a uprawnienia pracowników w systemach informatycznych nie wykraczały poza zakres określony w ich zakresach obowiązków. • Wprowadzono prawidłowe zabezpieczenia techniczne w systemach informatycznych w celu zapewnienia ochrony przetwarzanych informacji przed nieuprawnionym dostępem.	• Stwierdzono nieprawidłowości polegające w szczególności na: – nie w pełni rzetelnych analizach ryzyka w związku z potrzebą zachowania ciągłości działania systemów IT, – nieopracowaniu i niewdrożeniu kompletnego planu zapewnienia ciągłości działania oraz planów odtworzeniowych, – niepoddawaniu w okresie objętym kontrolą przeglądowi i aktualizacji dokumentacji SZBI, – braku kart uprawnień do systemów informatycznych dla trzech pracowników, – nieodebraniu dwóm osobom, które zakończyły pracę w urzędzie, uprawnień do poczty służbowej, – niewłaściwym zabezpieczeniu pomieszczenia serwerowni, – braku zapisów gwarantujących zachowanie odpowiedniego poziomu bezpieczeństwa informacji w dwóch umowach serwisowych – nie w pełni rzetelnych analizach ryzyka.

Lp.	Nazwa jednostki kontrolowanej	Ocena kontrolowanej działalności*/	Stany mające wpływ na wydaną ocenę:	
			prawidłowe	nieprawidłowe
			• Ustanowiono zasady (procedury) gwarantujące bezpieczną pracę przy pracy zdalnej, w szczególności przy przetwarzaniu mobilnym i pracy na odległość. • Przeprowadzono także szkolenia dla pracowników zaangażowanych w proces przetwarzania informacji oraz zapewniono przeprowadzenie audytu z zakresu bezpieczeństwa informacji.	
22.	Urząd Miejski w Nowej Rudzie	w formie opisowej	• Urząd nie zawsze prawidłowo i rzetelnie realizował zadania związane z zapewnieniem bezpieczeństwa informacji oraz ciągłości działania systemów informatycznych. • W szczególności w badanym okresie w urzędzie nie było w pełni wdrożonego Systemu Zarządzania Bezpieczeństwem Informacji. • Urząd nie posiadał również jednolitej dokumentacji w zakresie polityki bezpieczeństwa informacji. • Jednocześnie w tym okresie stosowano dokumentację składającą się na Politykę Ochrony Danych Osobowych w Urzędzie, uwzględniającą wymogi RODO. • W okresie objętym kontrolą prowadzono analizę ryzyka w związku z potrzebą zachowania ciągłości działania systemów informatycznych. Zidentyfikowane zostały kluczowe elementy infrastruktury i usługi IT, lecz nie nadano odpowiednich procentowych ważności kluczowym elementom, a także nie opisano planów naprawczych w przypadku wystąpienia awarii. • Urząd zapewnił właściwe rozwiązania zapobiegające możliwości instalacji nieautoryzowanego oprogramowania na urządzeniach służbowych oraz uniemożliwiające dostęp do danych na urządzeniach mobilnych. Jednocześnie wszystkie zweryfikowane umowy serwisowe posiadały zapisy gwarantujące odpowiedni poziom bezpieczeństwa. • W urzędzie opracowano plany ciągłości działania i plany odtworzeniowe, należy jednak podkreślić, że powinny one zawierać bardziej szczegółowe zapisy i wskazane byłoby uszczegółowienie dokumentacji w tym zakresie.	• Stwierdzono nieprawidłowości polegające na: – braku nadania zbiorom danych odpowiedniej ważności w procesie identyfikowania danych podlegających zabezpieczeniu, – nieprzeprowadzeniu przeglądu stanu bezpieczeństwa danych osobowych w terminie wymaganym regulacjami wewnętrznymi, – niezapoznaniu się większości pracowników z postanowieniami Regulaminu użytkownika komputerów przenośnych, – nieprzeprowadzaniu testów i treningów związanych z planami zapewnienia ciągłości działania, – niedokonywaniu przeglądu i aktualizacji dokumentacji zawierającej elementy polityki bezpieczeństwa informacji, – nieposiadaniu pełnych informacji o zasobach informatycznych urzędu, – niezablokowaniu kont w systemach IT byłym pracownikom urzędu, – ustaleniu wymogów dla haseł w systemach IT niezgodnie z wymogami stosowanej polityki haseł, – użytkowaniu pomieszczenia serwerowni w sposób niezapewniający odpowiedniej ochrony, – nieprawidłowym przechowywaniu nośników danych z kopiami zapasowymi, – nierealizowaniu szkoleń z zakresu bezpieczeństwa informacji, – wykonywaniu okresowego audytu wewnętrznego z zakresu bezpieczeństwa informacji z naruszeniem zasad niezależności i obiektywności.
23.	Starostwo Powiatowe w Kłodzku	w formie opisowej	• Starostwo nie zawsze prawidłowo i rzetelnie realizowało zadania związane z zapewnieniem bezpieczeństwa informacji oraz ciągłości działania systemów informatycznych. • W szczególności w badanym okresie w urzędzie nie było w pełni wdrożonego Systemu Zarządzania Bezpieczeństwem Informacji. • Urząd nie posiadał również jednolitej dokumentacji odnośnie polityki bezpieczeństwa informacji. • Jednocześnie w tym okresie stosowano dokumentację składającą się	• Stwierdzono nieprawidłowości polegające na: – braku nadania zbiorom danych odpowiedniej wagi istotności w procesie identyfikowania danych podlegających zabezpieczeniu, – nieprzeprowadzaniu analiz ryzyka związanych z potrzebą zachowania ciągłości działania systemów informatycznych; – nieopracowaniu polityki ciągłości działania, planu zapewnienia ciągłości działania oraz planu odtworzeniowego; – niedokonywaniu przeglądu i aktualizacji dokumentacji

Lp.	Nazwa jednostki kontrolowanej	Ocena kontrolowanej działalności*/	Stany mające wpływ na wydaną ocenę:	
			prawidłowe	nieprawidłowe
			na Politykę Ochrony Danych Osobowych, uwzględniającą wymogi RODO. • Wszystkie zweryfikowane umowy serwisowe posiadały zapisy gwarantujące odpowiedni poziom bezpieczeństwa. • Ustalono także zasady tworzenia i przechowywania kopii zapasowych, które to tworzono regularnie, a ich testowanie odbywało się automatycznie. • Nadawanie i odbieranie uprawnień pracownikom do pracy w systemach informatycznych odbywało się na podstawie wdrożonej w urzędzie procedury. • We wszystkich badanych przypadkach zablokowano konta w systemach informatycznych osobom, które zakończyły zatrudnienie. • Ponadto prawidłowo realizowano obowiązek przeprowadzania audytu wewnętrznego w zakresie bezpieczeństwa informacji. • Przeprowadzono także częściową analizę ryzyka utraty integralności, poufności oraz dostępności informacji. Należy jednak podkreślić, że niewystarczające było uwzględnienie ryzyk związanych ze zjawiskami atmosferycznymi czy też czynnikami zewnętrznymi, w związku z czym należy przeprowadzić ponowną analizę ryzyka dla całego obszaru IT.	zawierającej elementy polityki bezpieczeństwa informacji, – niezapobieżeniu możliwości zainstalowania nieautoryzowanego oprogramowania, – użytkowaniu pomieszczenia serwerowni w sposób niezapewniający odpowiedniej ochrony, – wyłączeniu Referatu Informatyki z administrowania zasobami sprzętowymi jak i oprogramowaniem jednego z wydziałów starostwa, – nieuwzględnieniu wszystkich etapów procedury identyfikacji kluczowych elementów infrastruktury i usług IT w procesie zapewnienia ciągłości działania; – nierealizowaniu wymaganych szkoleń z zakresu bezpieczeństwa informacji.
24.	Starostwo Powiatowe w Lubinie	w formie opisowej	• Starostwo nie zawsze prawidłowo i rzetelnie realizowało zadania związane z zapewnieniem bezpieczeństwa informacji oraz ciągłości działania systemów informatycznych. • W okresie objętym kontrolą stosowano dokumentację składającą się na System Zarządzania Bezpieczeństwem Informacji i Politykę Ochrony Danych Osobowych, uwzględniającą wymogi odpowiednio rozporządzenia KRI oraz RODO. • Ponadto w starostwie prawidłowo zidentyfikowano zbiory danych podlegających zabezpieczeniu oraz kluczowe elementy infrastruktury i usług IT. • Prowadzono także niezbędne analizy ryzyka oraz sporządzono odpowiednią dokumentację w celu m.in. zapewnienia ciągłości działania, określenia bezpiecznych zasad pracy zdalnej, określenia zasad tworzenia i przechowywania kopii zapasowych, nadawania i odbierania pracownikom uprawnień do pracy w systemach informatycznych oraz postępowania w sytuacjach wystąpienia lub podejrzenia wystąpienia incydentu w zakresie bezpieczeństwa informacji. • Właściwie wdrożono również rozwiązania organizacyjne i techniczne zapobiegające możliwości instalowania nieautoryzowanego oprogramowania oraz regularnie tworzono i testowano kopie zapasowe danych.	• Stwierdzono nieprawidłowości polegające na: – braku bieżącej aktualizacji SZBI wraz ze stwierdzanymi zmianami zachodzącymi w otoczeniu; – niezablokowaniu kont w systemach IT byłym pracownikom urzędu; – ustaleniu wymogów dla haseł w jednym z systemów informatycznych niezgodnie z wymogami SZBI; – niedostatecznym zabezpieczeniu pomieszczenia serwerowni; – braku w umowie na zakup sprzętu IT wraz z oprogramowaniem postanowień gwarantujących odpowiedni poziom bezpieczeństwa informacji; – braku realizacji szkoleń z zakresu bezpieczeństwa informacji; – przeprowadzeniu w 2023 r. okresowego, corocznego audytu wewnętrznego z zakresu bezpieczeństwa informacji z naruszeniem zasad niezależności i obiektywności.

*/ pozytywna/negatywna/w formie opisowej

6.2. ANALIZA STANU PRAWNEGO I UWARUNKOWAŃ ORGANIZACYJNO-EKONOMICZNYCH

Podstawowe wymagania w zakresie bezpieczeństwa informacji w jednostkach samorządu terytorialnego określają:

1) ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne[53],
2) obowiązujące od 23 maja 2024 r. rozporządzenie 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[54]. Wcześniejsze rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych[55] obowiązywało do 22 maja 2024 r.
3) ustawa z dnia 5 lipca 2018 r. o Krajowym Systemie Cyberbezpieczeństwa[56].

Wymagania dodatkowe znajdują się także w przepisach szczególnych, np. rozporządzeniu 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 dyrektyw 95/46/WE[57], tzw. RODO. Także w ustawie z dnia 29 września 1994 r. o rachunkowości[58], ustawie z dnia 6 września 2001 r. o dostępie do informacji publicznej[59], ustawie z dnia 15 kwietnia 2011 r. o systemie informacji oświatowej[60], ustawie z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną[61], można znaleźć przepisy odnoszące się do bezpieczeństwa informacji w danym obszarze.

Bezpieczeństwo informacji

System teleinformatyczny to zespół współpracujących ze sobą urządzeń informatycznych i oprogramowania zapewniający przetwarzanie, przechowywanie, a także wysyłanie i odbieranie danych przez sieci telekomunikacyjne za pomocą właściwego dla danego rodzaju sieci telekomunikacyjnego urządzenia końcowego w rozumieniu przepisów ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (art. 3 pkt 3 ustawy o informatyzacji). Minimalne wymagania dla systemów teleinformatycznych oznaczają zespół wymagań organizacyjnych i technicznych, których spełnienie przez system teleinformatyczny używany do realizacji zadań publicznych umożliwia wymianę danych z innymi systemami teleinformatycznymi używanymi do realizacji zadań publicznych oraz zapewnia dostęp do zasobów informacji udostępnianych za pomocą tych systemów (art. 3 pkt 9 ustawy o informatyzacji).

Zgodnie z art. 13 ust. 1 ustawy o informatyzacji, podmiot publiczny używa do realizacji zadań publicznych systemów teleinformatycznych spełniających minimalne wymagania dla systemów teleinformatycznych oraz zapewniających interoperacyjność systemów na zasadach określonych w Krajowych Ramach Interoperacyjności. W myśl art. 13 ust. 2 ustawy o informatyzacji, podmiot publiczny realizujący zadania publiczne przy wykorzystaniu systemu teleinformatycznego albo z użyciem środków komunikacji elektronicznej

[53] Dz. U. z 2024 r. poz. 1557, ze zm.
[54] Dz. U. poz. 773.
[55] Dz. U. z 2017 r. poz. 2247.
[56] Dz. U. z 2024 r. poz. 1077, ze zm.
[57] Dz. Urz. UE L 119 z 04.05.2016, str. 1, ze zm.
[58] Dz. U. z 2023 r. poz. 120, ze zm.
[59] Dz. U. z 2022 r. poz. 902.
[60] Dz. U. z 2024 r. poz. 152.
[61] Dz. U. z 2020 r. poz. 344.

do przekazywania danych pomiędzy tym podmiotem a podmiotem niebędącym organem administracji rządowej:

1) zapewnia, aby system teleinformatyczny służący do wymiany danych pomiędzy tym podmiotem a podmiotami niebędącymi organami administracji rządowej, poza minimalnymi wymaganiami, o których mowa w ust. 1, spełniał wymóg równego traktowania rozwiązań informatycznych;
2) publikuje w Biuletynie Informacji Publicznej lub udostępnia w inny sposób: zestawienie stosowanych w oprogramowaniu interfejsowym systemu teleinformatycznego używanego przez ten podmiot do realizacji zadań publicznych struktur dokumentów elektronicznych, formatów danych oraz protokołów komunikacyjnych i szyfrujących, oraz testy akceptacyjne, z zastrzeżeniem ust. 4.

Rozwiązania, o których mowa w ust. 2 pkt 2 lit. a, nie mogą wykraczać poza zakres minimalnych wymagań dla systemów teleinformatycznych (art. 13 ust. 3).

Na podstawie upoważnienia zawartego w art. 18 ustawy o informatyzacji wydane zostało obowiązujące od 23 maja 2024 r. rozporządzenie 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, a wcześniej rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych.

W myśl § 15 ust. 1 obowiązującego rozporządzenia 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.

Zarządzanie usługami realizowanymi przez systemy teleinformatyczne ma na celu dostarczanie tych usług na deklarowanym poziomie dostępności i odbywa się w oparciu o udokumentowane procedury (§ 15 ust. 2 obowiązującego rozporządzenia KRI). Wymagania określone w ust. 1 i 2 uznaje się za spełnione, jeśli projektowanie, wdrażanie, eksploatowanie, monitorowanie, przeglądanie, utrzymanie i udoskonalanie zarządzania usługą podmiotu realizującego zadanie publiczne odbywają się z uwzględnieniem Polskich Norm: PN-ISO/IEC 20000-1 i PN-ISO/IEC 20000-2 (§ 15 ust. 3 obowiązującego rozporządzenia KRI).

Zgodnie z załącznikiem nr 2 do obowiązującego rozporządzenia KRI, system teleinformatyczny używany do realizacji zadań publicznych musi obsługiwać standardy zapewniające dostęp do zasobów informacji oraz formaty danych określone w załączniku.

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. 1 obowiązującego rozporządzenia KRI).

Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności poprzez zapewnienie przez kierownictwo podmiotu publicznego warunków umożliwiających realizację i egzekwowanie działań wymienionych w § 19 ust. 2 obowiązującego rozporządzenia KRI w zakresie:

1) zapewnienia aktualizacji regulacji wewnętrznych w zakresie dotyczącym zmieniającego się otoczenia;
2) utrzymywania aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji obejmującej ich rodzaj i konfigurację;
3) przeprowadzania okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji oraz podejmowania działań minimalizujących to ryzyko, stosownie do wyników przeprowadzonej analizy;
4) podejmowania działań zapewniających, że osoby zaangażowane w proces przetwarzania informacji posiadają stosowne uprawnienia i uczestniczą w tym procesie w stopniu adekwatnym do realizowanych przez nie zadań oraz obowiązków mających na celu zapewnienie bezpieczeństwa informacji;
5) bezzwłocznej zmiany uprawnień, w przypadku zmiany zadań osób, o których mowa w pkt 4;
6) zapewnienia 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;
7) zapewnienia 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;
8) ustanowienia podstawowych zasad gwarantujących bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość;
9) zabezpieczenia informacji w sposób uniemożliwiający nieuprawnionemu jej ujawnienie, modyfikacje, usunięcie lub zniszczenie;
10) zawierania w umowach serwisowych podpisanych ze stronami trzecimi zapisów gwarantujących odpowiedni poziom bezpieczeństwa informacji;
11) ustalenia zasad postępowania z informacjami, zapewniających minimalizację wystąpienia ryzyka kradzieży informacji i środków przetwarzania informacji, w tym urządzeń mobilnych;
12) zapewnienia 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;
13) bezzwłocznego zgłaszania incydentów naruszenia bezpieczeństwa informacji w określony i z góry ustalony sposób, umożliwiający szybkie podjęcie działań korygujących;
14) zapewnienia okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji, nie rzadziej niż raz na rok.

Zgodnie z § 19 ust. 3 obowiązującego rozporządzenia KRI, obowiązki, o których mowa w § 19 ust. 1 i 2 uznaje się za spełnione, jeżeli system zarządzania bezpieczeństwem informacji został opracowany na podstawie Polskiej Normy PN-ISO/IEC 27001, a ustanawianie zabezpieczeń, zarządzanie ryzykiem oraz audytowanie odbywa się na podstawie Polskich Norm związanych z tą normą, w tym: PN-ISO/IEC 27002 – w odniesieniu do ustanawiania zabezpieczeń; PN-ISO/IEC 27005 – w odniesieniu do zarządzania ryzykiem.

Do 22 maja 2024 r. obowiązywało wcześniejsze rozporządzenie KRI. Obowiązki dotyczące opracowania, ustanowienia i wdrożenia SZBI były określone w § 20 wcześniejszego rozporządzenia KRI w sposób tożsamy jak w § 19 obowiązującego rozporządzenia KRI.

Ochrona danych osobowych

Od 25 maja 2018 r. obowiązuje unijne ogólne rozporządzenie o ochronie danych RODO.

W art. 5 RODO wskazuje podstawowe zasady ochrony danych osobowych. Wśród nich można wyróżnić następujące zasady:
- przetwarzania zgodnego z prawem, rzetelnego i przejrzystego,
- ograniczenia celu zbierania danych,
- minimalizacji danych,
- ograniczenia celu przetwarzania danych,
- prawidłowości przetwarzania danych,
- integralności i poufności przetwarzania,
- rozliczalności przetwarzania.

Art. 24 RODO określa obowiązki administratora[62]. Zgodnie z tym przepisem, uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia, administrator wdraża odpowiednie środki techniczne i organizacyjne, aby przetwarzanie odbywało się zgodnie z niniejszym rozporządzeniem i aby móc to wykazać. Środki te są w razie potrzeby poddawane przeglądom i uaktualniane (art. 24 ust. 1). Jeżeli jest to proporcjonalne w stosunku do czynności przetwarzania, środki, o których mowa w ust. 1, obejmują wdrożenie przez administratora odpowiednich polityk ochrony danych (art. 24 ust. 2). Stosowanie zatwierdzonych kodeksów postępowania, o których mowa wart. 40, lub zatwierdzonego mechanizmu certyfikacji, o którym mowa w art. 42, może być wykorzystane jako element dla stwierdzenia przestrzegania przez administratora ciążących na nim obowiązków (art. 24 ust. 3).

Zgodnie z art. 25 ust. 1 RODO, uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze wynikające z przetwarzania, administrator – zarówno przy określaniu sposobów przetwarzania, jak i w czasie samego przetwarzania – wdraża odpowiednie środki techniczne i organizacyjne, takie jak pseudonimizacja, zaprojektowane w celu skutecznej realizacji zasad ochrony danych, takich jak minimalizacja danych, oraz w celu nadania przetwarzaniu niezbędnych zabezpieczeń, tak by spełnić wymogi niniejszego rozporządzenia oraz chronić prawa osób, których dane dotyczą. Administrator wdraża odpowiednie środki techniczne i organizacyjne, aby domyślnie przetwarzane były wyłącznie te dane osobowe, które są niezbędne dla osiągnięcia każdego konkretnego celu przetwarzania. Obowiązek ten odnosi się do ilości zbieranych danych osobowych, zakresu ich przetwarzania, okresu ich przechowywania oraz ich dostępności. W szczególności środki te zapewniają, by domyślnie dane osobowe nie były udostępniane bez interwencji danej osoby nieokreślonej liczbie osób fizycznych (art. 25 ust. 2).

[62] Definicja pojęcia „administrator" została zawarta w art. 4 pkt 7 RODO.

W pkt 49 preambuły do RODO określono, iż przetwarzanie danych osobowych w zakresie bezwzględnie niezbędnym i proporcjonalnym do zapewnienia bezpieczeństwa sieci i informacji – tj. zapewnienia odporności sieci lub systemu informacyjnego na danym poziomie poufności na przypadkowe zdarzenia albo niezgodne z prawem lub nieprzyjazne działania naruszające dostępność, autentyczność, integralność i poufność przechowywanych lub przesyłanych danych osobowych – oraz bezpieczeństwa związanych z nimi usług oferowanych lub udostępnianych poprzez te sieci i systemy przez organy publiczne, zespoły reagowania na zagrożenia komputerowe, zespoły reagowania na komputerowe incydenty naruszające bezpieczeństwo, dostawców sieci i usług łączności elektronicznej oraz dostawców technologii i usług w zakresie bezpieczeństwa jest prawnie uzasadnionym interesem administratora, którego sprawa dotyczy. Może to obejmować na przykład zapobieganie nieuprawnionemu dostępowi do sieci łączności elektronicznej i rozprowadzaniu złośliwych kodów, przerywanie ataków typu „odmowa usługi", a także przeciwdziałanie uszkodzeniu systemów komputerowych i systemów łączności elektronicznej.

Zgodnie z art. 30 ust. 1 RODO, każdy administrator jest zobowiązany do prowadzenia rejestru czynności przetwarzania danych osobowych, za które odpowiada. W rejestrze tym zamieszcza się wszystkie informacje wyszczególnione w tym przepisie. Również podmiot, któremu powierzono przetwarzanie danych osobowych, zobowiązany jest do prowadzenia rejestru wszystkich kategorii czynności przetwarzania dokonywanych w imieniu administratora (art. 30 ust. 2 RODO). Rejestry te mają formę pisemną, w ramach której ustawodawca unijny przewiduje również formę elektroniczną (art. 30 ust. 3 RODO). Rejestr podlega obowiązkowi udostępnienia na żądanie organu nadzorczego.

Ponadto, pkt 82 preambuły do RODO wskazuje, że dla zachowania zgodności z niniejszym rozporządzeniem, administrator lub podmiot przetwarzający powinni prowadzić rejestry czynności przetwarzania, za które są odpowiedzialni. Każdy administrator i każdy podmiot przetwarzający powinni mieć obowiązek współpracować z organem nadzorczym i na jego żądanie udostępniać mu te rejestry w celu monitorowania tych operacji przetwarzania.

W myśl pkt 83 preambuły, w celu zachowania bezpieczeństwa i zapobiegania przetwarzaniu niezgodnemu z niniejszym rozporządzeniem administrator lub podmiot przetwarzający powinni oszacować ryzyko właściwe dla przetwarzania oraz wdrożyć środki – takie jak szyfrowanie – minimalizujące to ryzyko. Środki takie powinny zapewnić odpowiedni poziom bezpieczeństwa, w tym poufność, oraz uwzględniać stan wiedzy technicznej oraz koszty ich wdrożenia w stosunku do ryzyka i charakteru danych osobowych podlegających ochronie. Oceniając ryzyko w zakresie bezpieczeństwa danych, należy wziąć pod uwagę ryzyko związane z przetwarzaniem danych osobowych – takie jak przypadkowe lub niezgodne z prawem zniszczenie, utracenie, zmodyfikowanie, nieuprawnione ujawnienie lub nieuprawniony dostęp do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych – i mogące w szczególności prowadzić do uszczerbku fizycznego, szkód majątkowych lub niemajątkowych.

Bezpieczeństwo przetwarzania danych osobowych zostało uregulowane w art. 32 RODO. Zgodnie z ust. 1 niniejszego artykułu, uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia, administrator i podmiot przetwarzający mają obowiązek wdrożyć odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający temu ryzyku, w tym między innymi w stosownym przypadku:

a) pseudonimizację i szyfrowanie danych osobowych;
b) zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania;
c) zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego;
d) regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania (art. 32 ust. 1 RODO).

Oceniając, czy stopień bezpieczeństwa jest odpowiedni, uwzględnia się w szczególności ryzyko wiążące się z przetwarzaniem, w szczególności wynikające z przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych (art. 32 ust. 2 RODO).

Zgodnie z art. 32 ust. 3 RODO, wywiązywanie się przez administratora i podmiot przetwarzający z obowiązków, o których mowa w ust. 1, można wykazać między innymi poprzez stosowanie zatwierdzonego kodeksu postępowania, o którym mowa w art. 40 lub zatwierdzonego mechanizmu certyfikacji, o którym mowa w art. 42 RODO.

Artykuł 33 RODO reguluje zgłaszanie naruszenia ochrony danych osobowych organowi nadzorczemu. W przypadku naruszenia ochrony danych osobowych, administrator bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia – zgłasza je organowi nadzorczemu właściwemu zgodnie z art. 55, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych. Do zgłoszenia przekazanego organowi nadzorczemu po upływie 72 godzin dołącza się wyjaśnienie przyczyn opóźnienia (art. 33 ust. 1). Podmiot przetwarzający po stwierdzeniu naruszenia ochrony danych osobowych bez zbędnej zwłoki zgłasza je administratorowi (art. 33 ust. 2). Zgłoszenie, o którym mowa w ust. 1, musi co najmniej: opisywać charakter naruszenia ochrony danych osobowych, w tym w miarę możliwości wskazywać kategorie i przybliżoną liczbę osób, których dane dotyczą, oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie; zawierać imię i nazwisko oraz dane kontaktowe inspektora ochrony danych lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji; opisywać możliwe konsekwencje naruszenia ochrony danych osobowych; opisywać środki zastosowane lub proponowane przez administratora w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków (art. 33 ust. 3). Jeżeli – i w zakresie, w jakim – informacji nie da się udzielić w tym samym czasie, można je udzielać sukcesywnie bez zbędnej zwłoki (art. 33 ust. 4). Administrator dokumentuje wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze. Dokumentacja ta musi pozwolić organowi nadzorczemu weryfikowanie przestrzegania niniejszego artykułu (art. 33 ust. 5).

Zgodnie z art. 37 ust. 1 lit. a RODO, w przypadku gdy przetwarzania dokonują organ lub podmiot publiczny, administrator i podmiot przetwarzający wyznaczają zawsze inspektora ochrony danych. Status inspektora ochrony danych określa art. 38 RODO. Administrator oraz podmiot przetwarzający zapewniają, by inspektor ochrony danych był właściwie i niezwłocznie włączany we wszystkie sprawy dotyczące ochrony danych osobowych. Administrator oraz podmiot przetwarzający wspierają inspektora ochrony danych w wypełnianiu przez niego zadań, zapewniając mu zasoby niezbędne do wykonania tych zadań oraz dostęp

do danych osobowych i operacji przetwarzania, a także zasoby niezbędne do utrzymania jego wiedzy fachowej. Administrator oraz podmiot przetwarzający zapewniają, by inspektor ochrony danych nie otrzymywał instrukcji dotyczących wykonywania tych zadań. Nie jest on odwoływany ani karany przez administratora ani podmiot przetwarzający za wypełnianie swoich zadań. Inspektor ochrony danych bezpośrednio podlega najwyższemu kierownictwu administratora lub podmiotu przetwarzającego. Osoby, których dane dotyczą, mogą kontaktować się z inspektorem ochrony danych we wszystkich sprawach związanych z przetwarzaniem ich danych osobowych oraz z wykonywaniem praw przysługujących im na mocy niniejszego rozporządzenia. Inspektor ochrony danych jest zobowiązany do zachowania tajemnicy lub poufności co do wykonywania swoich zadań – zgodnie z prawem Unii lub prawem państwa członkowskiego. Inspektor ochrony danych może wykonywać inne zadania i obowiązki. Zgodnie z art. 38 ust. 6 RODO inspektor ochrony danych może wykonywać inne obowiązki, jednak najwyższe kierownictwo zapewnia by takie zadania i obowiązki nie powodowały konfliktu interesów.

Zgodnie z art. 39 RODO do zadań inspektora ochrony danych należy:

1) informowanie administratora, podmiotu przetwarzającego oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy niniejszego rozporządzenia oraz innych przepisów Unii lub państw członkowskich o ochronie danych i doradzanie im w tej sprawie;
2) monitorowanie przestrzegania niniejszego rozporządzenia, innych przepisów Unii lub państw członkowskich o ochronie danych oraz polityk administratora lub podmiotu przetwarzającego w dziedzinie ochrony danych osobowych, w tym podział obowiązków, działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty;
3) udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania zgodnie z art. 35;
4) współpraca z organem nadzorczym;
5) pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, o których mowa w art. 36, oraz w stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach.

Ustawa o krajowym systemie bezpieczeństwa

Zgodnie z art. 21 ustawy o ksc:

1) podmiot publiczny, o którym mowa w art. 4 pkt 7–15, realizujący zadanie publiczne zależne od systemu informacyjnego jest obowiązany do wyznaczenia osoby odpowiedzialnej za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa.
2) organ administracji publicznej może wyznaczyć jedną osobę odpowiedzialną za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa w zakresie zadań publicznych zależnych od systemów informacyjnych, realizowanych przez jednostki jemu podległe lub przez niego nadzorowane.
3) jednostka samorządu terytorialnego może wyznaczyć jedną osobę odpowiedzialną za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa w zakresie zadań publicznych zależnych od systemów informacyjnych, realizowanych przez jej jednostki organizacyjne.

Art. 22 ust. 1 pkt 5 ustawy o ksc przewiduje, że podmiot publiczny (...), realizujący zadanie publiczne zależne od systemu informacyjnego przekazuje do właściwego CSIRT MON, CSIRT NASK lub CSIRT GOV dane osoby, o której mowa w art. 21, obejmujące imię i nazwisko, numer telefonu oraz adres poczty elektronicznej, w terminie 14 dni od dnia jej wyznaczenia, a także informacje o zmianie tych danych w terminie 14 dni od dnia ich zmiany.

Ustawa z dnia 8 marca 1990 r. o samorządzie gminnym

Zgodnie z art. 6 ust. 1 ustawy o samorządzie gminnym[63] (dalej: usg), do zakresu działania gminy należą wszystkie sprawy publiczne o znaczeniu lokalnym, niezastrzeżone ustawami na rzecz innych podmiotów. Stosownie do art. 6 ust. 2 usg, jeżeli ustawy nie stanowią inaczej, rozstrzyganie w sprawach, o których mowa w ust. 1 art. 6, należy do gminy.

Według art. 7 ust. 1 usg zaspokajanie zbiorowych potrzeb wspólnoty należy do zadań własnych gminy, a w pkt 1–20 tego przepisu wymieniono jakie sprawy obejmują w szczególności zadania własne.

Zgodnie z art. 26 ust. 1 usg organem wykonawczym gminy jest wójt. Burmistrz jest organem wykonawczym w gminie, w której siedziba władz znajduje się w mieście położonym na terytorium tej gminy (art. 26 ust. 3 usg). W miastach powyżej 100 tys. mieszkańców organem wykonawczym jest prezydent miasta (art. 26 ust. 4 usg). Zgodnie z art. 11a ust. 3 usg, ilekroć w ustawie o gminach jest mowa o wójcie, należy przez to rozumieć także burmistrza oraz prezydenta miasta.

Wójt kieruje bieżącymi sprawami gminy oraz reprezentuje ją na zewnątrz (art. 31 usg). W myśl art. 33 ust. 1 usg, wójt wykonuje zadania przy pomocy urzędu gminy. Organizację i zasady funkcjonowania urzędu gminy określa regulamin organizacyjny, nadany przez wójta w drodze zarządzenia (art. 33 ust. 2 usg). Kierownikiem urzędu jest wójt. Wójt może powierzyć prowadzenie określonych spraw gminy w swoim imieniu zastępcy wójta lub sekretarzowi gminy (art. 33 ust. 3 i 4 usg). Kierownik urzędu wykonuje uprawnienia zwierzchnika służbowego w stosunku do pracowników urzędu oraz kierowników gminnych jednostek organizacyjnych (art. 33 ust. 5 usg).

Ustawa z dnia 5 czerwca 1998 r. o samorządzie powiatowym

W art. 4 ust. 1 w pkt 1–23 ustawy o samorządzie powiatowym[64] (dalej: usp) wymienione zostały zadania publiczne o charakterze ponadgminnym wykonywane przez powiat. Ustawy mogą określać inne zadania powiatu (art. 4 ust. 3 usp), a także mogą określać niektóre sprawy należące do zakresu działania powiatu jako zadania z zakresu administracji rządowej wykonywane przez powiat (art. 4 ust. 4 usp).

Organem wykonawczym powiatu jest zarząd powiatu (art. 26 ust. 1 usp). W skład zarządu powiatu wchodzą starosta jako jego przewodniczący, wicestarosta i pozostali członkowie (art. 26 ust. 2 usp).

Zgodnie z art. 33 usp, zarząd wykonuje zadania powiatu przy pomocy starostwa powiatowego oraz jednostek organizacyjnych powiatu, w tym powiatowego urzędu pracy. Starosta organizuje pracę zarządu powiatu i starostwa powiatowego, kieruje bieżącymi sprawami powiatu oraz reprezentuje powiat na zewnątrz (art. 34 ust. 1 usp). Stosownie do art. 35 ust. 1 usp, organizację i zasady funkcjonowania starostwa powiatowego określa regulamin organizacyjny. Starosta jest kierownikiem starostwa powiatowego oraz zwierzchnikiem służbowym pracowników starostwa i kierowników jednostek organizacyjnych powiatu oraz zwierzchnikiem powiatowych służb, inspekcji i straży (art. 35 ust. 2 usp).

W myśl art. 91 usp, prawa powiatu przysługują miastom, które w dniu 31 grudnia 1998 r. liczyły więcej niż 100 tys. mieszkańców, a także miastom, które z tym dniem przestały być siedzibami wojewodów, chyba że na wniosek właściwej rady miejskiej odstąpiono od nadania miastu praw powiatu, oraz tym, którym nadano status miasta na prawach powiatu, przy dokonywaniu pierwszego podziału administracyjnego kraju na powiaty.

[63] Dz. U. z 2024 r. poz. 1465, ze zm.
[64] Dz. U. z 2024 r. poz. 107.

Zgodnie z art. 92 ust. 1 usp, funkcje organów powiatu w miastach na prawach powiatu sprawuje rada miasta i prezydent miasta. Stosownie do art. 92 ust. 2 usp, miasto na prawach powiatu jest gminą wykonującą zadania powiatu na zasadach określonych w ustawie o powiatach. Ustrój i działania organów miasta na prawach powiatu, w tym nazwę, skład, liczebność oraz ich powoływanie i odwoływanie, a także zasady sprawowania nadzoru określa ustawa o samorządzie gminnym (art. 92 ust. 3 usp).

6.3. WYKAZ AKTÓW PRAWNYCH DOTYCZĄCYCH KONTROLOWANEJ DZIAŁALNOŚCI

1. Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne[65].
2. Ustawa z dnia 5 lipca 2018 r. o Krajowym Systemie Cyberbezpieczeństwa[66]
3. 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 dyrektyw 95/46/WE[67].
4. Rozporządzenie 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[68], obowiązujące od 23 maja 2024 r.
5. Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych[69], obowiązujące do 22 maja 2024 r.

[65] Dz. U. z 2024 r. poz. 1557, ze zm.
[66] Dz. U. z 2024 r. poz. 1077, ze zm.
[67] Dz. Urz. UE L 119 z 04.05.2016, str. 1, ze zm.
[68] Dz. U. poz. 773.
[69] Dz. U. z 2017 r. poz. 2247.

6.4. WYKAZ PODMIOTÓW, KTÓRYM PRZEKAZANO INFORMACJĘ O WYNIKACH KONTROLI

1. Prezydent Rzeczypospolitej Polskiej
2. Marszałek Sejmu Rzeczypospolitej Polskiej
3. Marszałek Senatu Rzeczypospolitej Polskiej
4. Prezes Rady Ministrów
5. Prezes Trybunału Konstytucyjnego
6. Rzecznik Praw Obywatelskich
7. Minister Cyfryzacji
8. Minister Spraw Wewnętrznych i Administracji
9. Przewodniczący Sejmowej Komisji Cyfryzacji, Innowacyjności i Nowoczesnych Technologii
10. Przewodniczący Sejmowej Komisji do Spraw Kontroli Państwowej
11. Przewodniczący Sejmowej Komisji Samorządu Terytorialnego i Polityki Regionalnej
12. Przewodniczący Senackiej Komisji Samorządu Terytorialnego i Administracji Państwowej
13. Prezydenci/Burmistrzowie/Wójtowie
14. Starostowie

Wiceprezes Rady Ministrów
Minister Cyfryzacji

Krzysztof Gawkowski

BM.WN.0810.8.2025
Warszawa, 12 marca 2025 r.

Pan
Marian Banaś
Prezes
Najwyższej Izby Kontroli

Szanowny Panie Prezesie,

w związku z art. 64 ust. 2 ustawy z dnia 23 grudnia 1994 r. o Najwyższej Izbie Kontroli[1], odnosząc się do Informacji o wynikach kontroli nr P/24/004 *Zapewnienie bezpieczeństwa informacji oraz ciągłości działania systemów informatycznych w jednostkach samorządu terytorialnego,* przedstawiam stanowisko dotyczące wniosków zawartych w przedmiotowej Informacji o wynikach kontroli.

Ad ***Biorąc pod uwagę skalę i zakres zidentyfikowanych nieprawidłowości, zasadne jest stałe wspieranie urzędów j.s.t przez Ministra Cyfryzacji w zakresie wdrażania rozwiązań organizacyjnych i technicznych dotyczących bezpieczeństwa informacji oraz zapewnienia ciągłości działania urzędów jst.***

MC[2] konsekwentnie buduje i rozwija krajowy system cyberbezpieczeństwa, aby zapewnić ochronę cyberprzestrzeni RP[3] na właściwym poziomie. Zapewnienie cyberbezpieczeństwa jest jednym z głównych priorytetów ministra cyfryzacji.

Jednym z ważnych elementów Krajowego Systemu Cyberbezpieczeństwa są JST[4].

W celu zwiększenia poziomu bezpieczeństwa informacji jednostek samorządu terytorialnego JST poprzez wzmacnianie odporności oraz zdolności do skutecznego zapobiegania i reagowania na incydenty w systemach informacyjnych w 2024 r. został uruchomiony specjalny program „Cyberbezpieczny Samorząd".

Projekt grantowy pn. „Cyberbezpieczny Samorząd" realizowany jest w ramach Programu Operacyjnego FERC[5] Działanie 2.2. pn. „Wzmocnienie krajowego systemu cyberbezpieczeństwa".

Projekt jest realizowany na terenie całego kraju. Zostały nim objęte wszystkie jednostki samorządowe, tj. 2 477 gminy, 314 powiatów oraz 16 województw.

W ramach programu podpisano 2 494 umowy na przyznanie grantów w wysokości od 200 000 zł do 850 000 PLN. Łącznie jednostki samorządu terytorialnego otrzymają pomoc na kwotę 1 473 239 856,33 PLN.

Celem Projektu grantowego pn. „Cyberbezpieczny Samorząd" jest zwiększenie bezpieczeństwa informacji poprzez wzmacnianie odporności jednostek samorządu terytorialnego oraz ich zdolności do skutecznego zapobiegania incydentom bezpieczeństwa teleinformatycznego, wykrywania ich i reagowania na nie.

[1] Ustawa z dnia 23 grudnia 1994 r. o Najwyższej Izbie Kontroli (Dz. U. z 2022 r. poz. 623).
[2] Ministerstwo Cyfryzacji
[3] Rzeczpospolita Polska.
[4] Jednostki samorządu terytorialnego.
[5] Fundusze Europejskie na Rozwój Cyfrowy 2021–2027.

telefon: +48 22 245 54 42
adres email: sekretariat.BM@cyfra.gov.pl
adres strony internetowej: www.gov.pl/cyfryzacja

adres: ul. Królewska 27
00-060 Warszawa

Tak postawiony cel jest szczególnie ważny w kontekście potencjalnych konsekwencji dotyczących zaniechań w tym obszarze, narażania instytucji na szkody, wstrzymania pracy urzędów, utraty danych czy mienia, ujawnienia wrażliwych danych osobom nieuprawnionym albo umożliwienia atakującym zniszczenia dokumentów lub danych.

Projekt poprzez wsparcie grantowe jednostek samorządowych, przyczyni się do:

- wdrożenia lub aktualizacji w JST polityk bezpieczeństwa informacji (SZBI - System Zarządzania Bezpieczeństwem Informacji),
- wdrożenia w JST środków zarządzania ryzykiem w cyberbezpieczeństwie,
- wdrożenia w JST mechanizmów i środków zwiększających odporność na ataki z cyberprzestrzeni,
- podniesienia poziomu wiedzy i kompetencji personelu JST kluczowego z punktu widzenia SZBI wdrożonego w urzędzie,
- przeprowadzenia w JST audytów SZBI potwierdzających uzyskanie wyższego poziomu odporności na cyberzagrożenia.

Działalność ministra cyfryzacji jest kierowana nie tylko do JST, ale także do jednostek z nimi powiązanymi. Obecnie trwają zawansowane prace nad Projektem - Wsparcie przedsiębiorstw wodociągowo-kanalizacyjnych, wykorzystujących technologie informacyjne (IT) oraz operacyjne (OT) stosowane w przemysłowych systemach sterowania (ICS) w modernizacji i rozbudowie infrastruktury cyberbezpieczeństwa w sieciach IT. Celem przedsięwzięcia jest poprawa cyberbezpieczeństwa podmiotów krajowego systemu cyberbezpieczeństwa. W ramach tego przedsięwzięcia przewiduje się objąć wsparciem min. 430 podmiotów. Każdy z wymienionych podmiotów będzie uprawniony do otrzymania wsparcia na poprawę odporności na cyberzagrożenia, w tym modernizację i rozbudowę infrastruktury cyberbezpieczeństwa. Przewidywany budżet wsparcia to – 328 500 000,00 PLN.

Poza wsparciem finansowym dla JST prowadzona jest szeroka działalność szkoleniowa. MC we współpracy z NASK[6] oraz partnerami Programu Współpracy w Cyberbezpieczeństwie (PWCyber) prowadzi szkolenia online z cyberbezpieczeństwa.

Celem szkoleń jest:

- podniesienie świadomości o cyberzagrożeniach wśród pracowników administracji, które są istotne dla utrzymania krytycznej działalności społecznej lub gospodarczej,
- wzmocnienie praktycznych umiejętności w zakresie wykrywania i reagowania na cyberataki,
- aktualizacja wiedzy o obowiązujących standardach i najlepszych praktykach cyberbezpieczeństwa.

W ramach Krajowego Systemu Cyberbezpieczeństwa objęto szkoleniem 4 800 pracowników JST, przede wszystkim w formule stacjonarnej, pt. „Jak dbać o cyberbezpieczeństwo w jednostkach samorządu terytorialnego?”

MC w celu dotarcia do jak największej liczby odbiorców sfinansowało przygotowanie pakietu materiałów edukacyjnych poświęconych podstawowym cyberzagrożeniom i zasadom cyberhigieny, który może znacząco pomóc instytucjom w podnoszeniu świadomości oraz zwiększaniu poziomu bezpieczeństwa w cyfrowym świecie. Pakiet edukacyjny zawiera praktyczne wskazówki dotyczące rozpoznawania i unikania najczęstszych zagrożeń, takich jak wiadomości phishingowe, złośliwe oprogramowanie czy dezinformacja. Zawiera również konkretne porady w zakresie codziennych praktyk cyberhigieny, takich jak zarządzanie hasłami, regularne aktualizacje oprogramowania czy bezpieczne korzystanie z internetu. Dzięki przystępnej formie i jasnym wyjaśnieniom,

[6] Naukowa i Akademicka Sieć Komputerowa – Państwowy Instytut Badawczy.

poradnik jest skierowany zarówno do specjalistów IT, jak i do pracowników, którzy nie mają technicznego wykształcenia, ale odgrywają kluczową rolę w ochronie danych organizacji.

MC zamierza w latach następnych kontynuować dotychczasowe formy wsparcia JST. Są przygotowywane nowe programy grantowe, jak i rozwijana jest forma szkoleń. W związku z dynamicznie zmieniającym się zakresem cyberzagrożeń, programy szkoleń wymagają bieżącej aktualizacji, aby zdolność do skutecznego zapobiegania i reagowania na incydenty w systemach informacyjnych była jak najwyższa.

Z wyrazami szacunku
Krzysztof Gawkowski
Wiceprezes Rady Ministrów
Minister Cyfryzacji
/dokument podpisany elektronicznie/

telefon: +48 22 245 54 42
adres email: sekretariat.BM@cyfra.gov.pl
adres strony internetowej: www.gov.pl/cyfryzacja

adres: ul. Królewska 27
00-060 Warszawa