RADA MIEJSKA W KĘTRZYNIE

KOMISJA REWIZYJNA

SPRAWOZDANIE Z KONTROLI

OCHRONA DANYCH OSOBOWYCH W GMINIE MIEJSKIEJ KĘTRZYN

Kętrzyn, wrzesień 2025

Podstawa prawna kontroli: Uchwała Rady Miejskiej w Kętrzynie Nr XII/89/2024 z dnia 30 grudnia 2024 r.

Okres objęty kontrolą:
Lata 2018-2025 r.

Cel kontroli: Celem kontroli ochrony danych osobowych w Gminie Miejskiej Kętrzyn jest weryfikacja zgodności działań gminy z przepisami RODO oraz innymi regulacjami prawnymi, w celu zapewnienia prawidłowości przetwarzania danych osobowych, zapobiegania ryzykom systemowym, ochrony praw i wolności osób fizycznych, a także zapewnienia wysokiego poziomu bezpieczeństwa danych.

Zespół kontrolujący:
Przewodniczący zespołu - radny Zbigniew Nowak
Członek zespołu – radna Marzena Gajek

Zakres kontroli:
1. Organizacja ochrony danych osobowych w Urzędzie Miasta Kętrzyn i jednostkach organizacyjnych miasta.
2. Rozwiązania w zakresie zapobiegania i przeciwdziałania zagrożeniom bezpieczeństwa informacji.
3. Naruszenia ochrony danych.

Kierownik kontrolowanej jednostki:
Burmistrz Miasta Kętrzyn Ryszard Niedziółka – w latach 2019 - kwiecień 2024 r.,
Karol Lizurej od 6.05.2024 r.

Komisja kontrolą objęła Urząd Miasta w Kętrzynie oraz wytypowane trzy jednostki organizacyjne: Przedszkole „Malinka", Miejski Ośrodek Pomocy Społecznej oraz Szkołę Podstawową Nr 5. Wyjaśnień Komisji w zakresie objętym przedmiotem kontroli udzielali: pracownicy Urzędu Miasta: Naczelnik Wydziału Organizacyjnego pani Marzena Mierzaniec, Inspektor pani Ewelina Marcinowska, informatycy: Adam Walukiewicz i Krzysztof Żukowski, Dyrektor MOPS Katarzyna Hoszkiewicz, Dyrektor SP 5 Bożena Mickiewicz oraz Dyrektor Przedszkola „Malinka" Joanna Friedrichsen. Komisja odbyła spotkanie także z Inspektorem Ochrony Danych panem Rafałem Andrzejewskim.

Skróty użyte w sprawozdaniu:

UODO - Urząd Ochrony Danych Osobowych
RODO - Rozporządzenie o ochronie danych osobowych Parlamentu Europejskiego i Rady (UE) z dnia 27 kwietnia 2016 r.
IOD – Inspektor Ochrony Danych
SZBI - System Zarządzania Bezpieczeństwem Informacji
PBI - Polityka Bezpieczeństwa Informacji
IT - (Information Technology) – technika informatyczna
GLPI - Menedżer Sprzętu IT
KRI - Krajowe Ramy Interoperacyjności
ASI – Administrator Systemów Informatycznych

Charakterystyka zagadnienia objętego kontrolą.

Urząd Miasta w Kętrzynie oraz jednostki organizacyjne Miasta realizując swoje zadania, gromadzą, wykorzystują i udostępniają bardzo wiele informacji dotyczących osób fizycznych. Przez wiele lat informacje te były gromadzone na nośnikach papierowych i były przetwarzane w sposób tradycyjny, co sprawiało, że ilość danych była ograniczona, dostęp do danych osobowych miało nieliczne grono osób, a efektywność procesów przetwarzania była niewielka. Od kilkunastu lat sytuacja w tym zakresie uległa radykalnej zmianie wskutek informatyzacji - zastosowania komputerów do przetwarzania danych w administracji publicznej. To nie tylko spowodowało wzrost ilości przetwarzanych danych czy wzrost efektywności procesów informacyjnych ale także wzrostu wielu zagrożeń związanych z przetwarzaniem danych takich jak: nieuprawnionym dostępem do danych, ich utratą i wielu innych niepożądanych skutków związanych ze zautomatyzowanym procesem ich przetwarzania. Wobec tego wyzwaniem stała się kwestia zapewnienia osobom, których dane poddawane są przetwarzaniu, ochrony przed negatywnymi skutkami wynikającymi z tego procesu.

Problematykę ochrony danych regulują:

a) 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 sprawie swobodnego przepływu takich danych (Dz. U. L 119).

b) ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (t. j. Dz. U. 2025, poz. 198)

c) 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 (Dz. U. z 2024, poz. 773).

d) § 3 i § 4 Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy Informatyczne służące do przetwarzania danych osobowych (Dz.U. Nr 100, poz. 1024).

Wyniki kontroli

1. Organizacja ochrony danych osobowych w Urzędzie Miasta i jednostkach Organizacyjnych Miasta.

Proces realizacji zadań w zakresie ochrony danych osobowych w Urzędzie Miasta Kętrzyn i jednostkach organizacyjnych Miasta rozpoczął się od wdrożenia odpowiednich działań organizacyjno-technicznych wynikających zarówno z ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (t. j. Dz. U. 2025 poz. 198), jak i Rozporządzenia Parlamentu Europejskiego i Rady UE 2016/679 z dnia 27 kwietnia 2016 r. (Dz. U. L 119). Celem tych działań było przede wszystkim zapewnienie bezpieczeństwa przetwarzanych informacji, które mają wpływ na bezpieczeństwo danych osobowych. Realizacja procesu rozpoczęta została od powołania zarządzeniem Nr 59/2018 z dnia 1 marca 2018 r. Zespołu ds. wdrażania wyżej cytowanego rozporządzenia Parlamentu Europejskiego. Celem prac Zespołu było przygotowanie koncepcji systemu ochrony danych osób fizycznych zgodnie z wymaganiami RODO. Zespół rozwiązany został z dniem 25 maja 2018 r.

Następnym działaniem było wyznaczenie Zarządzeniem Nr 154/2018 z 24 maja 2018 r. zarówno dla Urzędu Miasta, jak i jednostek organizacyjnych **Inspektora Ochrony Danych**. Obowiązek wyznaczenia IOD wynika z treści art. 37 ust. 1 RODO i obejmuje podmioty sektora finansów publicznych przetwarzających dane osobowe. W okresie 2019-30.06.2022

funkcję IOD realizowała pani Monika Zygmunt-Jakuć,"bezowijania" Sp. z o.o. w Warszawie, która powołana została zarządzeniem Burmistrza Miasta nr 154/2018 z 24 maja 2018 r. w sprawie wyznaczenia Inspektora Ochrony Danych Osobowych, natomiast od dnia 01.07.2022, Zarządzeniem Nr 194/2022 z dnia 1 lipca 2022 r wyznaczył pana Rafała Andrzejewskiego prowadzącego działalność pod nazwą: Ex Lege Szkolenia, Outsorsing Usług IOD. Podstawą wykonywania funkcji IOD są umowy: SO.271.1.84.2022, SO.272.1.22.23 z dnia19.06.2023, SO .272.1.16.2024 z dnia 27.06.2024 oraz aneksu Nr 1 do tej umowy do 31.12 2025. Zgodnie z umową wymieniony, jako IOD, świadczy usługi na rzecz Urzędu Miasta i jednostek organizacyjnych Miasta z zakresu ochrony danych osobowych oraz zadań przypisanych IOD wynikających z ustawy z dnia 10.05.2018 o ochronie danych osobowych oraz zadań wynikających z przepisów Rozporządzenia Parlamentu Europejskiego i Rady UE 2016/679 z 27.04.2016 r. Pan Rafał Andrzejewski posiada kwalifikacje oraz doświadczenie zawodowe, o których mowa w art. 37 ust. 5 RODO a w szczególności wiedzę fachową na temat prawa i praktyk w dziedzinie ochrony danych oraz umiejętności wypełnienia zadań, o których mowa w art. 39 RODO.

Zgonie z art. 39 RODO IOD czuwa nad wprowadzaniem przez Administratorów procesu ochrony danych oraz zaleceń wynikających z obowiązujących przepisów unijnych i krajowych w zakresie ochrony danych osobowych. Ponadto monitoruje przestrzeganie tych przepisów oraz polityk wprowadzanych w UM i JOM, prowadzi szkolenia pracowników, jak też wykonuje audyty z realizacji ochrony w UM i jednostkach wydając w razie konieczności stosowne zalecenia. Osobą wyznaczoną przez Burmistrza odpowiedzialną za wdrażanie zaleceń IOD oraz monitorowanie zagrożeń w Urzędzie Miasta jest pani Ewelina Marcinowska.

Zgodnie z obowiązującymi przepisami Burmistrz Miasta wprowadził zarządzeniami odpowiednie polityki ochrony danych i procedury ich przetwarzania a także monitorowania tego obszaru. Są to:

1. Zarządzenie Nr 155/2018 z dnia 24 maja 2018 r. w sprawie wprowadzenia Polityki Ochrony Danych Osobowych oraz Instrukcji Zarządzania Systemami Informatycznymi w Urzędzie Miasta.

2. Zarządzenie Nr 358/2020 z dnia 30.11.2020 mocą którego wprowadzono Politykę Bezpieczeństwa Informacji i Ochrony Danych Osobowych oraz Instrukcję Zarządzania Systemami Informatycznymi w Urzędzie Miasta Kętrzyn. Nadzór nad przestrzeganiem postanowień zawartych w tych dokumentach zarządzenie powierzało Inspektorowi Danych Osobowych. Jednocześnie zarządzenie uchyliło poprzednio wydane w tej sprawie zarządzenie nr 155/2018.

3. Zarządzenie Nr 63/2022 z dnia 28 marca 2022 r. w sprawie wprowadzenia Polityki Ochrony Danych osobowych w Straży Miejskiej w Kętrzynie.

4. Zarządzenie Nr 293/2022 z dnia 9 września 2022 r. wprowadzające u Administratora dokumentację ochrony danych tj.

- Politykę Ochrony Danych wraz z załącznikami oraz dokumenty wskazane w Polityce tj. „Politykę kluczy", „Politykę czystego ekranu" i „Politykę czystego biurka". Jednocześnie zarządzeniem tym uchylono zarządzenie nr 358/2020 z 30 listopada 2020 r. W dniu 31.05.2024 została zmieniona treść § 1 zarządzenia.

5. Na podstawie art. 24 ust. 1 i 2 oraz art. 32 RODO, Burmistrz Miasta zarządzeniem nr 314/2022 z 15 września 2022 r. wprowadził w Urzędzie Miasta następujące procedury z zakresu ochrony danych:

- ✓ procedura dopuszczenia osoby do pracy/współpracy/praktyki/stażu u administratora, która odnosi się do prowadzenia procesu rekrutacji i przyjmowania do pracy;
- ✓ procedura zarządzania zmianą, zapewnienia ochrony danych w fazie projektowania i domyślnej ochrony danych u administratora a także zapewnienia ciągłości zgodnie z zasadami Privacy by desing i Privacy by default;
- ✓ procedura oceny powagi naruszenia ochrony danych osobowych u administratora, której celem jest ocena poziomu naruszenia bezpieczeństwa danych osobowych celem zakwalifikowania zdarzenia wymagającego zgłoszenia lub nie do UODO;
- ✓ procedura realizacji praw osób fizycznych u administratora i dotyczy realizacji praw osób fizycznych oraz identyfikacji osób fizycznych występujących u Administratora z wnioskami lub żądaniami przysługującymi tym osobom w związku z przetwarzaniem danych osobowych;
- ✓ procedura wynoszenia dokumentacji wytworzonej u Administratora lub związanej z prowadzeniem działalności, a zawierające dane osobowe oraz wynoszenia sprzętu IT będącego w dyspozycji Administratora. Procedura dotyczy administratora systemów informatycznych, pracowników i współpracowników Administratora a także praktykantów, stażystów i wolontariuszy
- ✓ procedura korzystania ze sprzętu IT i systemów u administratora, która dotyczy podstawowych zasad jakimi kierować się powinien Administrator w zakresie przetwarzania danych osobowych w systemach informatycznych, nadawania uprawnień do korzystania ze sprzętu, metod i zasad uwierzytelniania użytkowników oraz zasad korzystania ze sprzętu IT, systemów, internetu i poczty elektronicznej;
- ✓ procedura zgłaszania incydentów u Administratora, która szczegółowo reguluje:
  - proces zgłaszania incydentów przez pracowników i kontrahentów Administratora,
  - dokonywania przez Administratora oceny czy dany incydent należy uznawać za naruszenia,
  - dokonywanie przez Administratora ocen czy dany incydent podlega zgłoszeniu do organu nadzoru;
- ✓ procedura prowadzenia ewidencji naruszeń ochrony danych osobowych, która zapewnia możliwość zgłaszania Administratorowi przez osoby fizyczne informacji o ewentualnych incydentach;
- ✓ procedura realizacji obowiązku informacyjnego względem klientów i kontrahentów oraz ich pracowników względem których Administrator zobowiązany jest realizować obowiązek informacyjny wynikający z kontaktów osobistych, korespondencji pocztowej, korespondencji za pomocą poczty elektronicznej i kontaktów telefonicznych.

6. Wypełniając postanowienia Rozporządzenia Rady Ministrów z 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności Burmistrz wydał zarządzeniem nr 319 z 20 września 2022 r. wprowadzając „Politykę Bezpieczeństwa Informacji" tym samym uchylając zarządzenie nr 358 z 30 listopada 2020 r.

7. Zarządzenie Nr 320/2022 z dnia 20 września 2022 r. wprowadzające do stosowania „Procedurę zarządzania incydentami bezpieczeństwa informacji", mającą na celu zapewnienie

ciągłości operacyjnej oraz ograniczanie wpływu przypadków naruszenia bezpieczeństwa zasobów informacyjnych.

8. Zarządzenie nr 336/2022 z dnia 5 października 2022 r. wprowadzające rejestr czynności przetwarzania danych osobowych. Rejestr prowadzony jest zarówno w formie papierowej, jak i elektronicznej.

W Urzędzie Miasta oraz w jednostkach organizacyjnych Miasta w latach 2018-2025 Administratorzy systematycznie wprowadzali niezbędne rozwiązania i zalecenia wynikające z obowiązujących przepisów a IOD raz w roku przeprowadzał audyty w zakresie zasad odnoszących się do bezpieczeństwa informacji i danych oraz efektywności wprowadzonych rozwiązań, przedstawiając wyniki w sprawozdaniach, które wskazują na to, iż stan zabezpieczenia systemu ochrony danych oraz wdrożone zabezpieczenia w Urzędzie Miasta i jednostkach organizacyjnych Miasta pozwalają na zapewnienie wymaganego poziomu ochrony. Dostęp do dokumentów i do pomieszczeń, w których przetwarzane są dane osobowe jest zastrzeżony tylko dla osób upoważnionych. Polityka ochrony danych osobowych spełnia wymagania RODO a obowiązek informacyjny w odniesieniu do osób, których dane dotyczą jest prawidłowo realizowany. Pracownicy znają zasady bezpiecznego przetwarzania danych. IOD, prowadząc bieżący monitoring realizacji zadań wynikających zarówno z Rozporządzenia, jak i z ustanowionych przez Administratora polityk nie stwierdzał naruszania przepisów o ochronie danych osobowych.

Stopień rozwiązań organizacyjnych i technicznych dostosowany był do wymogów rozporządzenia w sprawie Krajowych Ram Interoperacyjności i RODO. Jest on zadawalający, ale też wymagający ciągłych udoskonaleń. Administratorzy prawidłowo realizowali powierzanie przetwarzania danych określone w art. 28 RODO. Prawidłowo też określali obowiązki informacyjne oraz wzory tych obowiązków, zgodnie z art. 13 RODO. IOD sformułował jedno zalecenie dotyczące podjęcia działań zmierzających do wdrożenia na poziomie Urzędu Miasta systemowego rozwiązania dotyczącego zarządzania uprawnieniami do pracy w systemach informatycznych wykorzystywanych w Urzędzie Miasta.

Zarówno w Urzędzie Miasta i jednostkach organizacyjnych prawidłowo realizowano zadania dotyczące ustanowienia SZBI, które zapewniają właściwą ochronę informacji ale też ciągłe doskonalenie procedur w celu optymalizacji ryzyk, w tym PBI, która określa obowiązki pracowników, stosowane środki techniczne i organizacyjne. Z dokumentami tymi zapoznano pracowników Urzędu. W 2024 r. przeprowadzono również „Analizę zagrożeń i ryzyka przy przetwarzaniu danych osobowych" i opracowano „rejestr ryzyk", a także dokumentację z zakresu ochrony danych osobowych. Zapewniono odpowiednie zasoby kadrowe dla zachowania bezpieczeństwa informacji.

W okresie objętym kontrolą, przeprowadzono „Audyty bezpieczeństwa informacji w Urzędzie Miasta i jednostkach organizacyjnych Miasta Kętrzyn w zakresie zasad odnoszących się do bezpieczeństwa informacji i danych oraz efektywności wprowadzonych rozwiązań w zakresie zarządzania uprawnieniami pracowników. Z dokumentacji tych wynika, że wszelkie procedury związane z realizacją poszczególnych obszarów w ramach szeroko pojętej Polityki Bezpieczeństwa są prawidłowo realizowane. Obowiązuje także procedura wynoszenia dokumentacji wytworzonej w Urzędzie Miasta a także sprzętu IT będącego w dyspozycji

Urzędu, która wprowadzona została zarządzeniem Burmistrza Miasta Nr 314/2022 z dnia 15 września 2022 r.

Zasady wykonywania pracy zdalnej zostały opisane w „Regulaminie pracy zdalnej" wprowadzonym zarządzeniem Burmistrza Miasta Nr 77/2020 z dnia 27 marca 2020 r. w sprawie zasad organizacji pracy zdalnej w Urzędzie Miasta. W Regulaminie tym określono m.in. warunki dopuszczalności pracy zdalnej oraz zagadnienie ochrony informacji i danych osobowych. Warunkiem dopuszczalności pracy zdalnej było złożenie przez pracownika wniosku i otrzymanie zgody przełożonego na wykonywanie pracy zdalnej. Podstawą prawną wykonywania pracy zdalnej stanowił art. 3 ustawy z dnia 2 marca 2020 r. o szczególnych rozwiązaniach związanych z zapobieganiem, przeciwdziałaniem i zwalczaniem COVID-19, które zostało uchylone zarządzeniem Burmistrza Miasta Nr 94/2023 z dnia 24 kwietnia 2024 r.

W Urzędzie Miasta i jednostkach organizacyjnych prowadzona jest „Analiza zagrożeń i ryzyka przy przetwarzaniu danych osobowych", obejmująca analizę ryzyka utraty integralności, poufności lub dostępności informacji, co jest zgodne z § 20 ust. 2 pkt 3 rozporządzenia KRI. Sposób postępowania w przypadku wystąpienia incydentu naruszenia ochrony danych osobowych został opisany w przyjętej, w ramach Polityki ochrony danych osobowych, „Instrukcji postępowania w sytuacji naruszenia ochrony danych osobowych w Urzędzie Miasta Kętrzyna". Procedura uwzględniała postanowienia art. 33 i 34 RODO. Opracowana też jest procedura wynoszenia dokumentacji wytworzonej w Urzędzie Miasta a także sprzętu IT będącego w dyspozycji Urzędu, która wprowadzona została zarządzeniem Burmistrza Miasta Nr 314/2022 z dnia 15 września 2022 r. Realizowany też był proces szkolenia pracowników przez IOD w zakresie ochrony danych osobowych. Prowadzono również dodatkowe szkolenia z pracownikami jednostek, w których odnotowano incydenty naruszenia danych osobowych.

2. Działania w zakresie zapobiegania i przeciwdziałania zagrożeniom bezpieczeństwa informacji.

Organy administracji publicznej posługujące się systemami elektronicznymi obowiązane są zwracać uwagę na bezpieczeństwo przetwarzania danych oraz cały proces wykorzystywania informacji. Ponadto używanie urządzeń komunikacji elektronicznej zapewnia błyskawiczny kontakt pomiędzy organem a podmiotem korzystającym z usług administracji. Niezaprzeczalnym jest to, że odpowiedzialność za bezpieczeństwo przetwarzania informacji takich, jak dane osobowe spoczywa na organach administracji publicznej.

Obszar funkcjonowania systemów informatycznych regulują przepisy ustawy z 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa oraz ustawa z 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne, a także przepisy rozporządzenia Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych.

Urząd Miasta i jednostki organizacyjne Miasta posługują się systemami elektronicznego przetwarzania danych i informacji, które zapewniają błyskawiczny kontakt pomiędzy organem a podmiotem korzystającym z usług administracji. Zatem odpowiedzialność za bezpieczeństwo przetwarzania danych oraz cały proces wykorzystywania informacji spoczywa w Urzędzie

Miasta na Burmistrzu Miasta oraz w poszczególnych jednostkach organizacyjnych, którymi są Kierownicy jednostek. Burmistrz wyznaczył Adama Walukiewicza na Administratora Systemu Informatycznego (ASI), którego zadanie obejmuje zarządzanie infrastrukturą IT, zapewnienie bezpieczeństwa danych i systemów, rozwiązywanie problemów technicznych, wdrażanie nowych technologii oraz współpracę z Inspektorem Ochrony Danych w celu ochrony danych osobowych. Kluczowe zadaniem jest zapewnienie ciągłości działania systemów, monitorowanie sieci i serwerów, a także reagowanie na awarie i incydenty.

W Urzędzie prowadzony jest elektroniczny rejestr zasobów teleinformatycznych za pomocą systemu GLPI, który służy m.in. do zarządzania zasobami IT, w tym do inwentaryzacji sprzętu informatycznego oraz monitorowania dostępu do danego urządzenia i systemu informatycznego przez pracowników Urzędu. Zablokowana jest też możliwość instalacji przez użytkowników systemów informatycznych nieautoryzowanego oprogramowania na komputerach służbowych i tabletach. Nadawanie uprawnień użytkownikom systemów informatycznych Urzędu i jednostek organizacyjnych było dokumentowane w postaci wniosku o przyznanie uprawnień w systemach informatycznych oraz o wydanie upoważnienia do przetwarzania danych, co jest zgodne z przyjętą w tym zakresie „Procedurą zarządzania uprawnieniami do pracy w systemie informatycznym" i „Procedurą monitoringu i kontroli dostępu do zasobów teleinformatycznych, prowadzenia logów systemowych".

W Urzędzie Miasta i jednostkach organizacyjnych nie stosuje się specjalnego oprogramowania odpowiedzialnego za szyfrowanie danych na dyskach twardych komputerów przenośnych, co wymagane jest § 19 ust. 2 pkt 9 i 11 rozporządzenia KRI. Sprzęt komputerowy do serwisu oraz utylizacji reguluje „Procedura wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych". Zarówno w Urzędzie Miasta jak i jednostkach brak jest procedury tworzenia i testowania kopii zapasowych, którą należy opracować. Brak jest również procedury zarządzania pojemnością dysków twardych. Kopie zapasowe przechowywane są zarówno na serwerach Urzędu i jednostek organizacyjnych, jak i serwerach podmiotu zewnętrznego.

W związku z potrzebą zapewnienia ciągłości działania systemów informatycznych w Urzędzie opracowano 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 związku z tym Burmistrz zarządzeniem Nr 81/2023 wprowadził analizę zagrożeń i ryzyka w przetwarzaniu danych. W analizie tej zawarto prawdopodobieństwo wystąpienia zagrożenie, skutki naruszenia oraz sposoby postepowania z ryzykiem, jak również zalecenia dotyczące zminimalizowania ryzyka wystąpienia braku ciągłości działania systemów informatycznych w Urzędzie.

Zarówno w Urzędzie Miasta jak i jednostkach organizacyjnych do kontaktów z Krajowym Systemem Cyberbezpieczeństwa odpowiedzialni są pracownicy komórek informatycznych. Polityka „Czystego ekranu" realizowana jest zgodnie z wytycznymi określonymi w zarządzeniu Burmistrza. Pracownicy Referatu Informatyki prowadzili na bieżąco monitorowanie zasobów informatycznych, w tym wydajności i pojemności nośników pamięci systemów. Podejmowane były również działania w zakresie zwiększenia zasobów informatycznych, w szczególności serwerowni w związku z rosnącymi potrzebami. Zarówno Urząd Miasta jak i jednostki organizacyjne nie posiadają systemu **backupu** tzn. systemu do

tworzenia kopii zapasowych służącego do archiwizowania ważnych danych w celu ich ochron y przed utratą zarówno z powodu np. awarii sprzętu IT, przypadkowego usunięcia czy ataków cybernetycznych. System ten wprowadzony zostanie w ramach realizacji projektu „Cyberbezpieczny Samorząd".

Kluczowym elementem infrastruktury są serwerownie, których lokalizacja nie we wszystkich jednostkach spełnia standardy techniczne, określone w Rozporządzeniu Ministra Pracy i Polityki Socjalnej w sprawie ogólnych przepisów bezpieczeństwa i higieny pracy z dnia 26 września 1997 roku, a także innych przepisów odnoszących się do kwestii technicznych pomieszczeń, BHP czy ppoż. W Urzędzie serwerownia zlokalizowana przy wejściu do budynku Urzędu Miasta, której pomieszczenie nie odpowiada tym standardom. Różnie jest natomiast w przypadku jednostek organizacyjnych. Usprawiedliwieniem w tym przypadku są możliwości i warunki lokalowe budynków, w których mieści się zarówno Urząd Miasta jak i jednostki organizacyjne. Podejmowane są jednak działania w zakresie zapewnienia bezpieczeństwa informacji, m.in. poprzez zarówno zabezpieczenie serwerowni Urzędu przed nieuprawnionym dostępem, nadawanie uprawnień pracownikom adekwatnie do realizowanych przez nich zadań, uniemożliwienie zainstalowania przez pracowników nieautoryzowanego oprogramowania, zarządzanie pojemnością wykorzystywanych systemów informatycznych w sposób zapewniający właściwą ich wydajność. Wprowadzono również procedury dotyczące przekazywania sprzętu komputerowego podmiotom zewnętrznym, tworzenia i testowania kopii zapasowych.

Szeroko rozumiana Polityka Bezpieczeństwa Informacji, w ocenie Komisji, obejmuje również bezpieczeństwo obiektów, w których gromadzone i przetwarzane są dane podlegające prawnej ochronie. Obiektami tymi są zarówno Urząd Miasta, jak i budynki jednostek organizacyjnych. Budynek Urzędu Miasta przy ul. Wojska Polskiego objęty jest monitoringiem łącznie przez 10 kamer, z czego 4 kamery usytuowane są na poszczególnych kondygnacjach wewnątrz budynku oraz 6 kamer zewnętrznych, które monitorują teren wokół budynku. Natomiast budynek Urzędu Miasta przy Placu Piłsudskiego 1 monitorowany jest przez łącznie 4 kamery, z czego 3 kamery monitorują korytarze poszczególnych kondygnacji natomiast jedna kamera teren przed budynkiem.

W grudniu 2023 r. Gmina Miejska Kętrzyn złożyła wniosek o przystąpieniu do projektu „Cyberbezpieczny Samorząd", który dofinansowany jest ze środków UE na poziomie 82%. Umowa na realizację projektu podpisana została 18.07.2024 r. Wszystkie działania podjęte przez Gminę Miejską Kętrzyn w ramach projektu ukierunkowane są na: cyfrowy rozwój e-usług zwiększający katalog świadczonych usług poprzez internet, zwiększenie cyberbezpieczeństwa poprzez stosowanie zabezpieczeń organizacyjnych i technologicznych oraz wzmocnienie bezpieczeństwa poprzez pełne wdrażanie SZBI, co znacznie wpłynie na podniesienie na wyższy poziom i monitorowanie poziomu cyberbezpieczeństwa. Obecnie w Urzędzie Miasta i jednostkach nie jest wdrożony System Zarządzania Bezpieczeństwem Informacji w pełni spełniający wymogi KRI, co oczywiście ma istotny wpływ na zapewnienie bezpieczeństwa w obszarze cyberbezpieczeństwa.

W 2025 r. Miasto przystąpiło do realizacji projektu przygotowanego przez ASI Adama Walukiewicza utworzenia zintegrowanej infrastruktury informatycznej łączącej wszystkie jednostki organizacyjne oraz spółki komunalne z centralną serwerownią Urzędu Miasta. Dzięki

wykorzystaniu infrastruktury wytworzonej w ramach projektu „Cyberbezpieczny Samorząd" będzie można świadczyć profesjonalne usługi informatyczne dla wszystkich jednostek. Realizacje tego projektu umożliwi centralne zarządzanie bezpieczeństwem informatycznym wszystkich jednostek poprzez udostępnianie mocy obliczeniowych serwerów, wdrożenie jednolitego zarządzania domenowego z ujednoliconymi politykami dostępowymi oraz zabezpieczenie przed nieautoryzowanym ruchem sieciowym. Dodatkowo zostanie zapewniona profesjonalna architektura kopii zapasowych danych z aplikacji dziedzinowych oraz komputerów użytkowników, co znacząco podniesie poziom ochrony danych wrażliwych. Utworzenie scentralizowanego zespołu informatycznego składającego się z 3-4 specjalistów pozwoli w pełni zaspokoić zapotrzebowanie wszystkich jednostek na profesjonalną obsługę informatyczną, zastępując dotychczasowy model rozproszonych, często nieadekwatnych rozwiązań. W kolejnych etapach infrastruktura umożliwi wdrożenie internetu dla wewnętrznej komunikacji i obiegu dokumentów oraz aplikacji chmurowej do bezpiecznego udostępniania plików i organizacji spotkań online wykorzystującej darmowe oprogramowanie open-source. Szczególnie istotnym elementem będzie możliwość wdrożenia systemu EZD RP - bezpłatnego systemu elektronicznego zarządzania dokumentacją, który jest udostępniany przez NASK na zasadach niekomercyjnych dla jednostek administracji publicznej. Całkowity koszt inwestycji wynosi około 200 tysięcy złotych.

3. Naruszenia ochrony danych osobowych.

Procedura postępowania w przypadku naruszenia sytemu ochrony danych osobowych opisana została w Zarządzeniu Burmistrza Nr 320/2022 z dnia 20 września 2022 r., które wprowadziło „Procedurę zarządzania incydentami bezpieczeństwa informacji". Z przedstawionej Komisji dokumentacji wynika, że w okresie po wejściu w życie ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych, odnotowano w Urzędzie Miasta oraz jednostkach organizacyjnych łącznie **6** incydentów związanych z ujawnieniem chronionych danych, w tym **3** w 2021 oraz **3** w 2024 r.

1. Incydent zarejestrowany w dokumentacji pod nr 01/2021 miał miejsce 17.05.2021 i dotyczył naruszenia danych osobowych poprzez zamieszczenie na BIP części B oświadczenia majątkowego kierownika jednostki organizacyjnej Miasta, które oprócz imienia i nazwiska zawierało także inne dane podlegające ochronie kierownika jednostki organizacyjnej. Incydent został wyjaśniony dnia 20.05.2021 przez IOD, natomiast w analizie ryzyka incydent ten został zakwalifikowany jako pozbawienie kontroli na swoimi danymi osobowymi.

2. Incydent zarejestrowany pod nr 02/2021 dotyczył naruszenia danych osobowych w formie e-maila, zagubionego przez pracownika Biura Ludności Urzędu Miasta niewydanego właścicielowi dowodu osobistego. W tym przypadku incydent został wyjaśniony przez IOD. W ocenie ryzyka incydent został zakwalifikowany jako pozbawienie kontroli na swoimi danymi osobowymi.

3. Incydent zarejestrowany pod nr 03/2021 miał miejsce 20.08.2021 i polegał na dostarczeniu jednemu z kierowników jednostki organizacyjnej Miasta w niewłaściwie zabezpieczonej

kopercie dokumentacji zawierającej nie tylko jej dane osobowe ale też opis zdarzenia podlegające ochronie. Incydent zgłoszony został do IOD, który przeprowadził postępowanie wyjaśniające. Burmistrz Miasta wyciągnął wobec pracownika Urzędu, który naruszył przepisy o ochronie danych osobowych konsekwencje dyscyplinarne. W analizie ryzyka incydent został zakwalifikowany jako pozbawienie kontroli na swoimi danymi osobowymi.

4. W dniu 25.03.2024 r. zgłoszony został przez mieszkańca Kętrzyna incydent naruszenia danych osobowych poprzez zamieszczenie w dniu 22.03.2024 r. na stronie BIP Miasta Kętrzyn imienia i nazwiska oraz nr pesel. Administrator w dniu 25.03.2024 r. usunął zamieszczone dane a dnia 26.03.2024 r. zgłosił incydent do UODO. W dniu 27.03.2024 r. pismem nr DKN.5130.3316.2024. DJ Prezes UODO zalecił podjęcie działań zmierzających do eliminowania takich zdarzeń i rygorystycznego przestrzegania przepisów w obszarze ochrony danych osobowych. Burmistrz Miasta zainteresowanemu przedstawił stosowne wyjaśnienia.

5. W dniu 18.09.2024 r. ze skrzynki e-mailowej Szkoły Podstawowej Nr 5 wysłano e-maile, w których ujawniono 595 adresów i odbiorców, w tym: prywatne z imienia i nazwiska, 6 adresów z nickami i 556 firm i urzędów. Incydent został wykryty i zgłoszony przez Administratora do IOD, który wydał zalecenia naprawcze w postaci przeprowadzenia dodatkowego szkolenia z zakresu ochrony danych osobowych.

6. W dniu 27.09.2024 r. z konta malinka.ketrzyn@gmail.com wysłano maile do 181 odbiorców, ujawniając ich adresy e-mail, w tym: 26 prywatnych adresów z imienia i nazwiska, 28 adresów e-mail z nickami oraz 110 adresów e-mail firmowych i urzędowych. Informacja opisująca incydent przekazana został do IOD oraz do UODO w dniu 18.10.2024 r. IOD zalecił administratorowi przeprowadzenie dodatkowego przeszkolenia pracowników w zakresie ochrony danych osobowych, natomiast ze strony UODO zaleceń nie było.

Podsumowanie kontroli.

W okresie objętym kontrolą wdrożono w Urzędzie Miasta System Zarządzania Bezpieczeństwem Informacji, w ramach którego wprowadzono zarówno w Urzędzie, jak i jednostkach organizacyjnych, Politykę Bezpieczeństwa Informacji. Burmistrz Kętrzyna, zgodnie z wymaganiami określonymi w art. 37 RODO powołał Inspektora Ochrony Danych, którym w latach 2019-2022 była pani Monika Zygmunt-Jakuć a w od 1 lipca 2022, do dnia kontroli, pan Rafał Andrzejewski, posiadający przygotowanie merytoryczne i doświadczenie zawodowe do pełnienia tej funkcji. Od początku wejścia w życie zarówno ustawy z dnia 10 maja 2018 r o ochronie danych osobowych, jak i Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 26 kwietnia 2016 r. (RODO) wprowadzono i uaktualniano na bieżąco odpowiednie obszary i zagadnienia w ramach szeroko pojętej polityki bezpieczeństwa informacji. W ramach tych działań wprowadzono zasady tworzenia haseł dostępu do systemów informatycznych i zabezpieczenia uniemożliwiające instalowanie nieautoryzowanego oprogramowania.

Zorganizowano i systematycznie przeprowadzono w systemie e-learningowym szkolenia pracowników, po którym realizowany był przez IOD system testowy. Inspektor

Ochrony Danych przeprowadzał stosowne audyty poszczególnych obszarów dokonując oceny bezpieczeństwa i ochrony informacji. Zgodnie z art. 32 RODO opracowano analizę ryzyka jak również wprowadzono procedurę zarządzania incydentami naruszania bezpieczeństwa informacji. W latach 2019-2025 odnotowano łącznie 6 incydentów, które wyjaśniono i podjęto właściwe działania naprawcze. Pracownicy otrzymali adekwatne do realizowanych czynności uprawnienia do przetwarzania danych. Serwerownia znajdująca się w Urzędzie Miasta zajmuje pomieszczenie przy wejściu do Urzędu i nie spełnia standardów dla tego typu pomieszczenia i nie zabezpiecza w pełni przed nieuprawnionym dostępem.

W Urzędzie Miasta nie wdrożono klastera serwerów w celu zapewnienia ciągłości działania środowiska serwerowego Urzędu. Kopie zapasowe przechowuje się poza miejsce wytwarzania danych na zewnętrznych serwerach, co odpowiada warunkom przewidzianym w § 19 ust. 2 Rozporządzenia Rady Ministrów z 21 maja 2024 r. w sprawie Krajowym Ram Interoperacyjności.

W ocenie Komisji Burmistrz Miasta, jako Administrator Danych Osobowych a także kierownicy jednostek organizacyjnych w sposób prawidłowy wdrażali wszelkie procedury wynikające z RODO, co świadczy o przykładaniu dużej wagi do prawidłowego i zgodnego z obowiązującymi przepisami realizowania Polityki Bezpieczeństwa Informacji oraz Systemu Zarządzania Bezpieczeństwem Informacji zarówno w Urzędzie Miasta, jak i jednostkach organizacyjnych Miasta.

Komisja nie formułuje wniosków z uwagi na to, że aktualnie Miasto Kętrzyn realizuje projekt „Cyberbezpieczny Samorząd", którego celem jest standaryzacja procedur i polityk bezpieczeństwa w samorządach. Dzięki projektowi wprowadzone zostaną jednolite, wysokie standardy ochrony danych i systemów informatycznych oraz wzmocnione zdolności do szybkiego wykrywania i reagowania na incydenty a w konsekwencji wzmocniona zostanie ochrona danych osobowych mieszkańców, zwłaszcza w dobie rosnącej liczby cyberataków i wycieków danych. Projekt kładzie szczególny nacisk na wzrost zabezpieczenia wrażliwych informacji przetwarzanych przez Miasto Kętrzyn. Ponadto, jak wspomniano w sprawozdaniu, Miasto realizuje także projekt, stanowiący logiczną kontynuację inwestycji w cyberbezpieczeństwo, co zapewni Gminie Miejskiej Kętrzyn nowoczesną, scentralizowaną infrastrukturę informatyczną, zgodną z najwyższymi standardami bezpieczeństwa.

Sprawozdanie sporządzono w 3 jednobrzmiących egzemplarzach:
Egz. Nr 1 – Burmistrz Miasta Kętrzyn
Egz. Nr 2 – Rada Miejska
Egz. Nr 3 – a/a

Podpisy członków Komisji:

1. Zbigniew Nowak – przewodniczący .....
2. Ryszard Szymański – wiceprzewodniczący .....
3. Marzena Gajek – członek .....
4. Mateusz Lachowski .....