**WOJEWODA OPOLSKI**

Opole, dnia 30 grudnia 2024 r.
PN.I.431.4.1.2024.NL

**Pan**
**Tomasz Krupa**
**Burmistrz Gminy Baborów**
**Urząd Miejski w Baborowie**
**ul. Ratuszowa 2a**
**48-120 Baborów**

# WYSTĄPIENIE POKONTROLNE

## I. Dane identyfikacyjne kontroli

1. Nazwa i adres jednostki kontrolowanej: Urząd Miejski w Baborowie, ul. Ratuszowa 2a, 48-120 Baborów[1];
2. Podstawa prawna podjęcia kontroli:
   a) Art. 25 ust. 1 pkt 3 lit. a i ust. 3 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (t.j. Dz.U. z 2024 r. poz. 1557)[2],
   b) Art. 6 ust. 4 pkt 3 ustawy z dnia 15 lipca 2011 r. o kontroli w administracji rządowej (t.j. Dz.U z 2020 r. poz.224)[3];
3. Zakres kontroli:
   a) Przedmiot kontroli: Działanie systemów teleinformatycznych i rejestrów publicznych używanych do realizacji zadań zleconych z zakresu administracji rządowej,

[1] Dalej: UM w Baborowie
[2] Dalej: ustawa o informatyzacji działalności podmiotów
[3] Dalej: ustawa o kontroli

b) Okres objęty kontrolą: od 1 stycznia 2024 r. do dnia rozpoczęcia kontroli (z uwzględnieniem okresu wcześniejszego i późniejszego w zakresie niezbędnym do realizacji celu kontroli);

4. Rodzaj kontroli: problemowa;
5. Tryb kontroli: zwykły;
6. Termin kontroli: 21 października 2024 r. – 5 listopada 2024 r., kontrola prowadzona była w trybie hybrydowym, tj. dnia 22 października 2024 r. – rozpoczęcie czynności kontrolnych w UM w Baborowie oraz oględziny serwerowni na miejscu w jednostce. Pozostałe dni (21 października 2024 r. oraz 23 października – 5 listopada 2024 r. ) kontrola prowadzona była zdalnie;
7. Skład zespołu kontrolnego:
   a) Natalia Lenart – Inspektor Wojewódzki w Oddziale Organizacji, Kontroli i Skarg w Wydziale Prawnym i Nadzoru w Opolskim Urzędzie Wojewódzkim – kierownik zespołu kontrolnego,
   b) Agnieszka Orlińska-Gocka - Inspektor Wojewódzki w Oddziale Organizacji, Kontroli i Skarg w Wydziale Prawnym i Nadzoru w Opolskim Urzędzie Wojewódzkim – członek zespołu kontrolnego,
   c) Kamil Dziechciński - Starszy Specjalista w Oddziale Informatyki i Rozwoju w Biurze Obsługi Urzędu w Opolskim Urzędzie Wojewódzkim – członek zespołu kontrolnego;
8. Kierownik jednostki kontrolowanej: Pan Tomasz Krupa – Burmistrz Gminy Baborów, od dnia 6 maja 2024 r.

[akta kontroli, str. 2]

9. Kontrolę wpisano do książki kontroli prowadzonej w jednostce kontrolowanej, pod poz. nr 4/2024 (dokonano wpisu zastępczego).

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

Działanie systemów teleinformatycznych i rejestrów publicznych używanych do realizacji zadań zleconych z zakresu administracji rządowej, w okresie od 1 stycznia 2024 r. do dnia rozpoczęcia kontroli (z uwzględnieniem okresu wcześniejszego i późniejszego w zakresie niezbędnym do realizacji celu kontroli), tj. 21 października 2024 r. w Urzędzie Miejskim w Baborowie ocenia się pozytywnie z nieprawidłowościami.

W trakcie kontroli zostały stwierdzone nieprawidłowości oraz uchybienia, które zostały opisane poniżej.

W kontrolowanym okresie zakres działania i zadania oraz organizację i zasady funkcjonowania Urzędu Miejskiego w Baborowie określał Regulamin organizacyjny Urzędu Miejskiego w Baborowie[4] stanowiący załącznik nr 1 do Zarządzenia nr OW-391/23 Burmistrza Gminy Baborów w sprawie regulaminu organizacyjnego Urzędu Miejskiego w Baborowie.

W § 7 pkt 1 i 2 rozdziału 3 dot. zasad kierowania Urzędem zawartym w Regulaminie organizacyjnym, kierownikiem Urzędu jest Burmistrz, który kieruje pracą przy pomocy Zastępcy Burmistrza, Sekretarza i Skarbnika.

[akta kontroli, str. 61-63]

Osobą powołaną na funkcję Administratora Systemów Informatycznych[5] jest Pracownik ds. informatycznych Referatu Administracji i Ochrony Środowiska Urzędu Miejskiego w Baborowie, od 9 września 2019 roku.

[akta kontroli, str. 58]

Pracownikami odpowiedzialnymi ze strony UM w Baborowie za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa są Pracownik ds. informatycznych Referatu Administracji i Ochrony Środowiska oraz Sekretarz Gminy. Zgłoszenie osób do CSIRT NASK nastąpiło dnia 25 lutego 2021 roku.

[akta kontroli, str. 59-60]

Z informacji przekazanych podczas kontroli wynika, że w UM w Baborowie do realizacji zadań zleconych z zakresu administracji rządowej wykorzystywane są 4 systemy teleinformatyczne:

1. CEIDG (Centralna Ewidencja i Informacja o Działalności Gospodarczej) – jest to elektroniczny rejestr przedsiębiorców działających w Polsce. Portal pozwala na założenie firmy, aktualizację danych, a także na zawieszenie, wznowienie lub zamknięcie działalności gospodarczej. Dodatkowo wykorzystywany jest do przekazywania informacji o wydanych zezwoleniach, koncesjach oraz wpisach do rejestrów.
2. WOW (Wsparcie Organów Wyborczych) – jest informatycznym systemem pozwalającym na zarządzanie danymi oraz drukowanie dokumentacji dot. wyborów, takich jak: zaświadczenia o wyborze, obwieszczenia, projekty uchwał komisji wyborczych oraz postanowienia komisarzy. Wskazany system nie podlicza wyników głosowania. Zadanie to należy do obwodowych stacji

[4] Dalej: Regulamin organizacyjny
[5] Dalej: ASI

wyborczych, które po podpisaniu protokołu wprowadzają dane do systemu. Głównym jego zadaniem jest weryfikacja wprowadzonych informacji i wykrywanie błędów, a także niezwłocznie alarmowanie o ich zaistnieniu. System posiada również aplikację, dzięki której terytorialne komisje wyborcze sprawdzają prawidłowość policzenia wyników oraz rozdzielenia mandatów.

3. SRP (System Rejestrów Państwowych) – to system organizacyjno-techniczny wykorzystywany do prowadzenia rejestrów publicznych, na podstawie art. 13b ust. 1 ustawy o informatyzacji działalności podmiotów. Przedmiotowy system jest połączeniem najważniejszych polskich rejestrów, tj. Rejestr PESEL, Rejestr Dowodów Osobistych, Rejestr Dokumentów Paszportowych, Rejestr Stanu Cywilnego, Rejestr Danych Kontaktowych, System Odznaczeń Państwowych, Centralny Rejestr Sprzeciwów, Centralny Rejestr Wyborców, a także Rejestr zastrzegania numerów PESEL.
4. WyDra – jest to system mający na celu obsługę wszystkich podatków, opłat za gospodarowanie odpadami komunalnymi oraz innymi opłatami lokalnymi, w ramach jednego systemu. Dodatkowo system ten pozwala na wielokrotne wykorzystanie raz wprowadzonych danych, a także umożliwia analizę stanu dochodów jednostki samorządu terytorialnego na szeroką skalę. W przypadku UM w Baborowie system WyDra stosowany jest do wprowadzania wniosków akcyzowych, wydawania decyzji i generowania sprawozdań.

[akta kontroli, str. 104-105]

**1. Elektroniczna skrzynka podawcza**

Podstawa prawna:

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

UM w Baborowie posiada Elektroniczna Skrzynkę Podawczą[6]: /u90vj9hn3n/SkrytkaESP, znajdującą się na Elektronicznej Platformie Usług Administracji Publicznej[7], pozwalającą na wysyłanie i odbieranie pism w formie dokumentów elektronicznych. Na stronie głównej Biuletynu Informacji Publicznej[8] UM w Baborowie podano adres ESP, a na portalu internetowym UM w Baborowie zamieszczono bezpośredni odnośnik do ePUAP. Ponadto na stronie BIP Baborów

[6] Dalej: ESP
[7] Dalej: ePUAP
[8] Dalej: BIP

zamieszczony jest wykaz formatów danych przyjmowanych za pośrednictwem ESP, są to:

- Dane zawierające dokumenty tekstowe lub tekstowo graficzne: TXT, DOC, RTF, XLS, PDF, PPT, XPS, ODT, ODS, ODP, DOCX, XLSX, PTTX, CSV;
- Grafika: JPG(JPEG), TIF(TIFF), GEOTIFF, PNG, SVG;
- Dane zawierające informację dźwiękową lub filmową: WAV, MP3, AVI, MPG, MPEG, MP4, M4A, MPEG4, OGG, OGV;
- Dane skompresowane: ZIP, TAR, GZ(GZIP), 7Z.

[informacje z BIP Baborów, akta kontroli, str. 99]

**2. Obieg dokumentów elektronicznych w urzędzie**

Podstawa prawna:

- § 19 ust. 2 pkt 9 Rozporządzenia Rady Ministrów z dnia 21 maja 2024 r. w sprawie krajowych ram interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych[9]: Zarządzanie bezpieczeństwem informacji[10] realizowane jest w szczególności przez: zabezpieczenie informacji w sposób uniemożliwiający nieuprawnionemu jej ujawnienie, modyfikacje, usunięcie lub zniszczenie.

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

Podstawowym sposobem dokumentowania przebiegu załatwiania i rozstrzygania spraw w UM w Baborowie jest papierowy system wykonywania czynności kancelaryjnych. System elektroniczny pełni rolę systemu wspomagającego. W ramach zarządzania obiegiem dokumentacji w Urzędzie wykorzystywany jest system Elektronicznego Zarządzania Dokumentacją (EZD), PROTON - Nefeni.

[akta kontroli, str. 504]

[9] Dz.U. z 2024 r. poz. 773, dalej: Rozporządzenie KRI
[10] Dalej: BI

Zasady i procedury zarządzania i administrowania systemem informatycznym w UM w Baborowie w zakresie przetwarzania danych osobowych zostały określone w Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Miejskim w Baborowie[11] stanowiącej element Polityki Bezpieczeństwa Danych Osobowych w Urzędzie Miejskim w Baborowie[12] wprowadzonej Zarządzeniem nr KJ-39/23 Burmistrza Gminy Baborów z dnia 30 listopada 2023 r. w sprawie wprowadzenia Polityki Bezpieczeństwa Danych Osobowych w Urzędzie Miejskim w Baborowie[13].

[akta kontroli, str. 119-127]

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

Podstawa prawna:

- § 19 ust. 1 rozporządzenie KRI: Podmiot realizujący zadania publiczne opracowuje i ustanawia, wdraża i eksploatuje, monitoruje i przegląda oraz utrzymuje i doskonali system zarządzania bezpieczeństwem informacji zapewniający poufność, dostępność i integralność informacji z uwzględnieniem takich atrybutów, jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność;
- § 19 ust. 2 rozporządzenie KRI Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienie przez kierownictwo podmiotu publicznego warunków umożliwiających realizację i egzekwowanie działań związanych z bezpieczeństwem informacji;
- § 19 ust. 2 pkt 1 rozporządzenie KRI: Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez: zapewnienie aktualizacji regulacji wewnętrznych w zakresie dotyczącym zmieniającego się otoczenia.

Zgodnie z zapisami rozporządzenia KRI, podmiot publiczny realizujący zadania publiczne powinien opracować dokumentację Systemu Zarządzania Bezpieczeństwem Informacji[14], w tym regulacje wewnętrzne oraz zapewnienie ich aktualizacji zgodnie ze zmieniającym się otoczeniem. Kompleksowa dokumentacja SZBI jest warunkiem niezbędnym do skutecznego zarządzania bezpieczeństwem informacji w Urzędzie.

[11] Dalej: Instrukcja zarządzania systemem informatycznym
[12] Dalej: PBDO
[13] Dalej: Zarządzenie w sprawie wprowadzenia PBDO
[14] Dalej: SZBI

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

- Polityka bezpieczeństwa teleinformatycznego;
- Polityka bezpieczeństwa fizycznego;
- Polityka bezpieczeństwa danych osobowych;
- Procedura zarządzania ryzykiem;
- Regulamin korzystania z zasobów informatycznych;
- Procedura zarządzania sprzętem i oprogramowaniem;
- Procedura zarządzania konfiguracją;
- Procedura zarządzania uprawnieniami do pracy w systemach teleinformatycznych;
- Procedura monitorowania poziomu świadczenia usług;
- Procedura bezpiecznej utylizacji sprzętu elektronicznego;
- Procedura zarządzania zmianami i wykonywania testów;
- Procedura stosowania środków kryptograficznych;
- Procedura określania specyfikacji technicznych wymagań odbioru systemów IT;
- Procedura zgłaszania i obsługi incydentów naruszenia bezpieczeństwa informacji;
- Procedura wykonywania i testowania kopii bezpieczeństwa;
- Procedura monitoringu i kontroli dostępu do zasobów teleinformatycznych, prowadzenia logów systemowych.

Dodatkową dokumentację SZBI stanowią także:

- Dokumentacja z przeglądów SZBI;
- Dokumentacja z szacowania ryzyka bezpieczeństwa informacji;
- Dokumentacja postępowania z ryzykiem;
- Dokumentacja akceptacji ryzyka;

[15] Dalej: PBI

- Dokumentacja audytów z zakresu BI;
- Dokumentacja incydentów naruszania BI;
- Dokumentacja zarządzania uprawnieniami do pracy w systemach teleinformatycznych;
- Dokumentacja zarządzania sprzętem i oprogramowaniem teleinformatycznym;
- Dokumentacja szkolenia pracowników zaangażowanych w proces przetwarzania informacji.

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

W trakcie kontroli ustalono, że w UM w Baborowie nie został opracowany, ustanowiony i wdrożony System Zarządzania Bezpieczeństwem Informacji. Z wyjaśnień złożonych przez Burmistrza Gminy Baborów wynika, że „Wykonanie pełnej dokumentacji SZBI i jej wdrożenie planuje się na rok 2025 w ramach Projektu Cyberbezpieczny Samorząd. Pierwotnie planowano zrobić to w tym roku, ale przeciągające się procedury związane z Projektem Cyberbezpieczny Samorząd spowodowały przesunięcie terminu na 2025 rok z przyczyn obiektywnych". Załącznikami do złożonych wyjaśnień są: zapytanie ofertowe, opis przedmiotu zamówienia, formularz ofertowy oraz projekt umowy dotyczące, m.in. opracowania i aktualizacji dokumentacji SZBI w oparciu o KRI, normę ISO27001, określenia procedur postępowania związanych z BI.

[akta kontroli, str. 99, 438-490, 498, 500-501]

Obecnie w UM w Baborowie stosowana jest Polityka Bezpieczeństwa Danych Osobowych, która została opracowana na podstawie Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119, s. 1)[16]. Na PBDO składają się następujące dokumenty:

- Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Miejskim w Baborowie[17];

[16] Dalej: Rozporządzenie w sprawie RODO
[17] Dalej: Instrukcja zarządzania systemem informatycznym

- Środki organizacyjne i techniczne niezbędne dla zapewnienia poufności, integralności i rozliczalności danych osobowych w Urzędzie Miejskim w Baborowie[18];
- Procedura nadawania, zmiany i odwołania upoważnień do przetwarzania danych osobowych w Urzędzie Miejskim w Baborowie[19];
- Procedura zarządzania uprawnieniami w Urzędzie Miejskim w Baborowie[20]
- Procedura zabezpieczania danych osobowych w Urzędzie Miejskim w Baborowie[21];
- Instrukcja postępowania w przypadku zagrożenia lub naruszenia ochrony danych osobowych w Urzędzie Miejskim w Baborowie[22];
- Procedura zarządzania incydentami związanymi z bezpieczeństwem informacji i cyberbezpieczeństwem w Urzędzie Miejskim w Baborowie[23];
- Instrukcja postępowania na wypadek awarii systemu informatycznego w Urzędzie Miejskim w Baborowie[24];
- Procedura działań korygujących i zapobiegawczych w Urzędzie Miejskim w Baborowie[25];
- Plan ciągłości działania w Urzędzie Miejskim w Baborowie[26];
- Procedura zarządzania ryzykiem w Urzędzie Miejskim w Baborowie[27];
- Kontrola wewnętrzna stanu ochrony danych osobowych w Urzędzie Miejskim w Baborowie[28];
- Warunki dostępu podmiotu zewnętrznego do systemów lub zasobów teleinformatycznych w Urzędzie Miejskim w Baborowie[29];
- Procedura inicjacji i realizacji fazy planowania;
- Zasady udostępniania danych w Urzędzie Miejskim w Baborowie[30] wraz z załącznikiem nr 1 – Wykaz udostępnień danych osobowych innym podmiotom i załącznikiem nr 2 - Wykaz udostepnień danych osobom, których dotyczą;
- Polityka retencji;

[18] Dalej: Środki organizacyjne i techniczne niezbędne dla bezpieczeństwa danych osobowych
[19] Dalej: Procedura nadawania, zmiany i odwołania upoważnień
[20] Dalej: Procedura zarządzania uprawnieniami
[21] Dalej: Procedura zabezpieczania danych osobowych
[22] Dalej: Instrukcja postępowania w przypadku zagrożenia lub naruszenia ochrony danych osobowych
[23] Dalej: Procedura zarządzania incydentami
[24] Dalej: Instrukcja postępowania na wypadek awarii systemu informatycznego
[25] Dalej: Procedura działań korygujących i zapobiegawczych
[26] Dalej: Plan ciągłości działania
[27] Dalej: Procedura zarządzania ryzykiem
[28] Dalej: Kontrola wewnętrzna stanu ochrony danych osobowych
[29] Dalej: Warunki dostępu podmiotu zewnętrznego do systemów lub zasobów teleinformatycznych
[30] Dalej: Zasady udostępniania danych

- Procedura realizacji praw osób, których dane dotyczą w Urzędzie Miejskim w Baborowie[31] wraz z załącznikiem nr 1 – Wniosek o realizację praw osoby, której dane dotyczą;
- Procedura przewarzania danych szczególnych (wrażliwych) w Urzędzie Miejskim w Baborowie[32];
- Polityka haseł w Urzędzie Miejskim w Baborowie[33];
- Procedura postępowania z kluczami w Urzędzie Miejskim w Baborowie[34];
- Zasady korzystania z Internetu w Urzędzie Miejskim w Baborowie[35];
- Zasady korzystania z poczty elektronicznej w Urzędzie Miejskim w Baborowie[36];
- Regulamin postępowania z niechcianymi danymi osobowymi;
- Polityka czystego biurka i czystego ekranu w Urzędzie Miejskim w Baborowie[37];
- Regulamin funkcjonowania monitoringu wizyjnego w Urzędzie Miejskim w Baborowie[38];
- Procedura monitoringu GPS w samochodach służbowych Urzędu Miejskiego w Baborowie[39];
- Procedura przeglądu i usuwania danych osobowych przetwarzanych w związku z gospodarowaniem środkami zakładowego funduszu świadczeń socjalnych wraz z załącznikiem nr 1 – Sprawozdanie z rocznego przeglądu danych osobowych zgromadzonych w Zakładowym Funduszu Świadczeń Socjalnych;
- Załącznik do Zarządzenia w sprawie wprowadzenia PBDO – Obszar przetwarzania danych osobowych w Urzędzie Miejskim w Baborowie;
- Załącznik do Zarządzenia w sprawie wprowadzenia PBDO – Oświadczenie pracownika o zapoznaniu się z Polityką Bezpieczeństwa Danych Osobowych w Urzędzie Miejskim w Baborowie.

Polityka Bezpieczeństwa Danych Osobowych wraz z wszystkimi ją stanowiącymi dokumentami wymienionymi powyżej tworzą Politykę Bezpieczeństwa Informacji[40].

Zgodnie z zapisami PBDO każdy z pracowników przed dopuszczaniem do pracy przy użyciu systemu informatycznego jest zobowiązany do zapoznania

[31] Dalej: Procedura realizacji praw osób, których dane dotyczą
[32] Dalej: Procedura przewarzania danych szczególnych
[33] Dalej: Polityka haseł
[34] Dalej: Procedura postępowania z kluczami
[35] Dalej: Zasady korzystania z Internetu
[36] Dalej: Zasady korzystania z poczty elektronicznej
[37] Dalej: Polityka czystego biurka i czystego ekranu
[38] Dalej: Regulamin funkcjonowania monitoringu wizyjnego
[39] Dalej: Procedura monitoringu GPS w samochodach służbowych
[40] Dalej: PBI

się z przedmiotowym dokumentem. W związku z powyższym zwrócono się do Burmistrza Gminy Baborów o przedstawienie dokumentu potwierdzającego zapoznanie się z PBI przez pracowników Urzędu, stanowiącego załącznik do Zarządzenia w sprawie wprowadzenia PBDO. W odpowiedzi otrzymano przedmiotowe oświadczenia 4 wybranych pracowników UM w Baborowie losowo wraz z informacją, że „Dokument Oświadczenie pracownika o zapoznaniu się z Polityką Bezpieczeństwa Informacji w Urzędzie Miejskim w Baborowie wypełnia każdy pracownik przed objęciem obowiązków po przyjęciu do pracy i przechowywany jest w teczce osobowej pracownika (…)”**.**

[akta kontroli, str. 106-211, 500]

W związku z naruszeniem § 19 ust. 1 i 2 rozporządzenia KRI, tj. brakiem opracowania, ustanowienia, wdrożenia i eksploatowania, monitorowania i przeglądania oraz utrzymania i doskonalenia Systemu Zarządzania Bezpieczeństwem Informacji, w powyższym zakresie stwierdza się nieprawidłowość.

**4. Analiza zagrożeń związanych z przetwarzaniem informacji**

Podstawa prawna:

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

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

Z dokumentacji przedstawionej kontrolerom wynika, że ostatnia analiza ryzyka utraty integralności, dostępności lub poufności informacji była przeprowadzona w dniu 26 czerwca 2023 r, podczas której zostały określone ryzyka ogólne oraz te wymagające wprowadzenia określonego planu postępowania.

[akta kontroli, str. 212-231]

Z wyjaśnień złożonych przez Burmistrza Gminy Baborów wynika, że „… w miesiącu listopadzie 2024 roku przed planowanym audytem zostanie przeprowadzona analiza ryzyka systemów IT za 2024 rok".

[akta kontroli, str. 497]

**5. Inwentaryzacja sprzętu i oprogramowania informatycznego**

Podstawa prawna:

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

Zarządzenie infrastrukturą informatyczną wymaga utrzymywania aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji obejmującej ich rodzaj i konfigurację. W przedmiotowym spisie winny być wykazane wszystkie zidentyfikowane aktywa informatyczne wraz z najistotniejszymi informacjami, tj. szczegółowe dane o urządzeniach technicznych, oprogramowaniu i środkach komunikacji, ich rodzaju, parametrach, aktualnej konfiguracji i relacjach między elementami konfiguracji oraz użytkowniku. Stworzona baza ma na celu podejmowanie właściwych decyzji i działań w zakresie zmian w środowisku teleinformatycznym.

Zgodnie z zapisami § 3 pkt 4 i 5 Procedury zabezpieczania danych osobowych, bieżąca konserwacja sprzętu prowadzona jest tylko przez ASI, natomiast poważne naprawy wykonywane przez personel zewnętrzy odbywają się w siedzibie UM w Baborowie. Dodatkowo ASI dopuszcza konserwację i naprawę sprzętu poza siedzibą Urzędu wyłącznie po trwałym usunięciu danych. Zużyty sprzęt może być zbywalny dopiero po trwałym usunięciu danych, a urządzenia uszkodzone powinny być przekazywane właściwym podmiotom w celu ich utylizacji.

[akta kontroli, str. 138]

Jak wynika z analizy przedkontrolnej UM w Baborowie inwentaryzacja sprzętu odbywa się w aplikacji Środki Trwałe oraz zgodnie z wyjaśnieniami „rozliczalność nośników zewnętrznych do tej pory zapewniona była w systemie zarządzania

[redacted](…) System zapewnia bieżący wgląd kto posługuje się nośnikiem kiedy i na jakiej stacji roboczej go używał. (…) System pozwala użyć nośnika tylko przypisanemu użytkownikowi i tylko na stacji do której jest przypisany.”

[akta kontroli, str. 100, 297-298, 498]

Kontrolującym została przedstawiona dokumentacja potwierdzająca przeprowadzenie inwentaryzacji sprzętu zawierająca Zarządzenie Nr KJ-39/21 Burmistrza Gminy Baborów z dnia 8 października 2021 roku w sprawie przeprowadzenia inwentaryzacji składników majątkowych Gminy Baborów w 2021 roku, dokument potwierdzający powołanie Zespołów Spisowych do przeprowadzenia inwentaryzacji poszczególnych składników majątkowych wraz z wytycznymi, arkusze spisu z natury oraz protokół z inwentaryzacji środków trwałych i pozostałych środków trwałych.

[akta kontroli, str. 232-285]

Jednakże zespół kontrolerów nie uzyskał dokumentacji potwierdzającej przeprowadzenie inwentaryzacji oprogramowania służącego do przetwarzania informacji.

Ponadto Burmistrz Gminy Baborów złożył wyjaśnienia w zakresie braku sporządzania dokumentu potwierdzającego przekazanie pracownikowi nośnika zewnętrznego, z których wynika, że „W dniu 22.10.2024 r. zostały wygenerowane i podpisane przez użytkowników Protokoły przekazania sprzętu zewnętrznych nośników danych. (…) Obecnie będzie stosowana zasada przekazywania nośników zewnętrznych tylko na podstawie wydrukowanego i podpisanego protokołu.”

W związku z powyższym zostały stwierdzone nieprawidłowości w zakresie braku posiadania dokumentacji potwierdzającej przekazanie pracownikowi nośnika zewnętrznego oraz przeprowadzenie inwentaryzacji oprogramowania.

[akta kontroli, str. 498, 287-296]

**6. Zarządzanie uprawnieniami do pracy w systemach informatycznych**

Podstawa prawna:

- § 19 ust. 2 pkt 4 rozporządzenie KRI: Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez: podejmowanie działań zapewniających, że osoby zaangażowane w proces przetwarzania informacji posiadają stosowne uprawnienia i uczestniczą w tym procesie w stopniu

adekwatnym do realizowanych przez nie zadań oraz obowiązków mających na celu zapewnienie bezpieczeństwa informacji;

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

Kluczowym elementem polityki BI jest zarządzanie dostępem do systemów teleinformatycznych przetwarzających informacje. Zarządzenie dostępem ma zapewnić, że osoby zaangażowane w proces przetwarzania informacji posiadają stosowne uprawnienia i uczestniczą w tym procesie w stopniu adekwatnym do realizowanych przez nie zadań oraz obowiązków, a w przypadku zmiany zadań lub zakończenia stosunku pracy następuje zmiana lub odebranie uprawnień.

Zasady zarządzania uprawnieniami w systemach informatycznych określone zostały w § 3 Instrukcji zarządzania systemem informatycznym oraz w Procedurze zarządzania uprawnieniami stanowiące element PBDO.

[akta kontroli, str. 120-121, 133-136]

Ponadto w UM w Baborowie w zakresie upoważnień do przetwarzania danych została wprowadzona Procedura nadawania, zmiany i odwołania upoważnień do przetwarzania danych osobowych, a także rejestr osób posiadających wskazane upoważnienia.

[akta kontroli, str. 299-301, 131-132]

Z wyjaśnień Burmistrza Gminy Baborów wynika, że „ w kontrolowanym okresie nie było ruchów kadrowych w kontrolowanych referatach wobec czego nie było zmian dotyczących przyznania lub odebrania uprawnień pracownikom zajmującym się realizacją zadań zleconych z zakresu administracji rządowej (…)”

[akta kontroli, str. 502]

Jednakże z dokumentacji przekazanej kontrolerom wynika, że w przypadku konieczności modyfikacji uprawnień sporządzane są zgłoszenia odebrania uprawnień do przetwarzania danych osobowych w systemach informatycznych. Dodatkowymi informacjami zawartymi we wskazanych pismach są: data i powód odebrania upoważnienia do przetwarzania danych osobowych oraz data i adnotacja o odebraniu uprawnień przez osobę odpowiedzialną za zarządzanie uprawnieniami w systemie informatycznym.

[akta kontroli, str. 302-305]

Osobom posiadającym dostęp do danych osobowych wydawane są zarówno pisemne upoważnienia, jak i pisemne potwierdzenia nadania uprawnień

w systemach informatycznych do ich przetwarzania wraz z określeniem przypisanego systemu. Jednocześnie należy nadmienić, że w upoważnieniach do przetwarzania danych osobowych, znajdują się zapisy dot. zbiorów (systemu teleinformatycznego) do pracy, w którym dany pracownik jest upoważniony.

Z analizy dokumentacji wynika, że osobom posiadającym upoważnienia do przetwarzania danych osobowych nadano uprawnienia do przetwarzania danych osobowych w systemach informatycznych po 2 latach od uzyskania przez nich przedmiotowych upoważnień. W zakresie tym Burmistrz Gminy Baborów wyjaśnił, że „uprawnienia do przetwarzania danych osobowych w systemach informatycznych które Państwu przesłaliśmy są aktualizacją z bieżącego roku dostosowującą do wymogów Zarządzenia Nr KJ-39/236 Burmistrza Gminy Baborów z dnia 30 listopada 2023 roku. Każdy pracownik nowo zatrudniony otrzymuje upoważnienie do przetwarzania danych osobowych oraz uprawnienie do systemów informatycznych."

[akta kontroli, str. 7-10, 19-22, 27-30, 36-38, 44-46, 53-55, 504-505]

**7. Szkolenia pracowników zaangażowanych w proces przetwarzania informacji**

Podstawa prawna:

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

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

Z informacji podanych przez UM w Baborowie wynika, że szkolenia z zakresu cyberbezpieczeństwa przeprowadzane są raz w roku. Ostatnie takie szkolenie odbyło się w czerwcu 2023 roku i zgodnie z informacją z UM w Baborowie „kolejne

szkolenie z zakresu cyberbezpieczeństwa planowane jest 19 grudnia 2024 roku (…)". W dokumentacji z kontroli znalazła się lista obecności z kursu w przedmiotowym zakresie, zgodnie z którą wszyscy pracownicy zatrudnieni w tamtym okresie w Urzędzie odbyli szkolenie. Dodatkowo przeprowadzane są także szkolenia stanowiskowe dla pracowników.

[akta kontroli, str. 100, 306, 505]

W związku z brakiem informacji o częstotliwości przeprowadzanych szkoleń w zakresie danych osobowych, zwrócono się o złożenie wyjaśnień, z których wynika, że „ (…) ostatnie zbiorcze szkolenie dla pracowników Urzędu Miejskiego w Baborowie odbyło się 18 lutego 2021 roku. Szkolenia dla nowo zatrudnionych pracowników prowadzone są cyklicznie przy przyjęciu do pracy przez Inspektora Ochrony Danych z którym mamy podpisaną umowę. Kolejne zbiorcze szkolenie planowane jest w I kwartale 2025 roku." Przeprowadzenie ostatniego szkolenia z zakresu ochrony danych osobowych w 2021 zostaje stwierdzone jako uchybienie.

[akta kontroli, str. 505]

Dodatkowo w przesłanych dokumentach wykazane zostały zakresy tematyczne szkoleń dot. ochrony danych osobowych oraz cyberbezpieczeństwa.

[akta kontroli, str. 307, 502]

Po analizie dokumentacji ustalono, że osoby upoważnione do przetwarzania danych osobowych zostały przeszkolone w zakresie ochrony danych osobowych oraz cyberbezpieczeństwa, co potwierdzają właściwe dokumenty.

[akta kontroli, str. 11-12, 23-24, 31-32, 39-40, 47-48, 56-57]

W związku z udziałem UM w Baborowie w programie „Cyberbezpieczny Samorząd", zespół kontrolny poprosił o przedstawienie planu działań realizacji projektu. W odpowiedzi Burmistrz Gminy Baborów przekazał dokumentację złożoną z zapytania ofertowego, opisu przedmiotu zamówienia, formularza ofertowego oraz projektu umowy dotyczące m.in. szkoleń pracowników z zakresu cyberbezpieczeństwa w 2024, 2025 i 2026 roku.

[akta kontroli, str. 438-490, 500-501]

**8. Praca na odległość i mobilne przetwarzanie danych**

Podstawa prawna:

- § 19 ust. 2 pkt 8 rozporządzenie KRI: Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez: ustanowienie podstawowych zasad

gwarantujących bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość.

Zasady pracy zdalnej wraz z prawami i obowiązkami pracodawcy i pracownika zostały określone w Regulaminie wykonywania pracy w systemie pracy zdalnej przez pracowników Urzędu Miejskiego w Baborowie[41] stanowiącym załącznik nr 1 do Zarządzenia nr 11/2021 Burmistrza Gminy Baborów z dnia 21 marca 2021 r. w sprawie wprowadzenia Regulaminu wykonywania pracy w systemie pracy zdalnej przez pracowników Urzędu Miejskiego w Baborowie[42]. Dodatkową dokumentację w zakresie wykonywania pracy zdalnej stanowią:

- Oświadczenie pracownika wykonującego obowiązki służbowe w systemie pracy zdalnej, w tym także zobowiązanie do przetwarzania danych wyłącznie w miejscu wykonywania pracy stanowiące załącznik nr 2 do Zarządzenia w sprawie wprowadzenia Regulaminu wykonywania pracy zdalnej;
- Analiza ryzyka dla operacji przetwarzania danych realizowanych zdalnie w Urzędzie Miejskim w Baborowie;
- Procedura – Zasady organizacji pracy poza miejscem jej stałego wykonywania zwiększające bezpieczeństwo przetwarzania danych osobowych, stanowiąca uzupełnienie Regulaminu wykonywania pracy w systemie pracy zdalnej.

[akta kontroli, str. 308-323]

Powyższa dokumentacja wykonywania pracy w trybie zdalnym została opracowana w 2021 i opiera się na ustawie z dnia 2 marca 2020 r. o szczególnych rozwiązaniach związanych z zapobieganiem, przeciwdziałaniem i zwalczaniem COVID-19, innych chorób zakaźnych oraz wywołanych nimi sytuacji kryzysowych (t.j. Dz.U. z 2024 r. poz. 340 ze zm.).

Ponadto zostały opracowane zasady przetwarzania danych osobowych na komputerach przenośnych, które określono w Instrukcji zarządzania systemem informatycznym.

[akta kontroli, str. 123]

W związku z brakiem dokumentacji potwierdzającej wypożyczenie sprzętu komputerowego przez pracownika przechodzącego na pracę zdalną, zespół kontrolny poprosił o wyjaśnienia. Wynika z nich, że „ (…) pracownicy realizujący pracę zdalną posiadają sprzęt przydzielony do osobistego użytku poza siecią LAN Urzędu.”

[41] Dalej: Regulamin wykonywania pracy zdalnej
[42] Dalej: Zarządzenie w sprawie wprowadzenia Regulaminu wykonywania pracy zdalnej

W kontrolowanym okresie wystąpił jeden przypadek zlecenia pracy zdalnej pracownikowi UM w Baborowie. Z uwagi na wykonywanie przez wspomnianą osobę zadań niewiązanych z zadaniami zleconymi z zakresu administracji rządowej, nie został on poddany kontroli.

[akta kontroli, str. 324-336, 498-499]

Dodatkowo z uwagi na nieaktualną podstawę prawną dokumentacji dotyczącej wykonywania pracy zdalnej, Burmistrz Gminy Baborów zadeklarował, że „w związku ze stwierdzeniem w czasie kontroli problemowej nieaktualności Zarządzenia Burmistrza Gminy dot. pracy zdalnej przygotowano nowe Zarządzenie Burmistrza. (…) Po podpisaniu przez Burmistrza zostanie niezwłocznie wdrożony w Urzędzie Miejskim w Baborowie.” Projekt nowego zarządzenia w sprawie ustalenia Regulaminu wykonywania pracy zdalnej został przesłany jako załącznik do składanych wyjaśnień.

Stosowanie Regulaminu wykonywania pracy zdalnej na podstawie nieaktualnych przepisów prawnych, stwierdzone zostaje jako nieprawidłowość.

[akta kontroli, str. 337-356, 499]

**9. Serwis sprzętu informatycznego i oprogramowania**

Podstawa prawna:

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

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

Wytyczne dotyczące zawierania umów serwisowych ze stronami trzecimi zawarte są w części PBDO – Warunki dostępu podmiotu zewnętrznego do systemów lub zasobów teleinformatycznych.

[akta kontroli, str. 165-169]

UM w Baborowie wykorzystuje jeden system teleinformatyczny przeznaczony do realizacji zadań zaleconych z zakresu administracji rządowej zakupiony u zewnętrznego dostawcy. W związku z tym została podpisana stosowana umowa

licencyjna, umożliwiająca prawidłową eksploatację i rozwój poprzez zgłaszanie występujących błędów oraz świadczenie pomocy przez dystrybutora. Dodatkowo zawarta została stosowana umowa powierzenia przetwarzania danych osobowych gwarantująca właściwe zabezpieczenie danych w przypadku awarii systemu, a także zapewniająca bezpieczeństwo przetwarzanych informacji uzyskanych przez wykonawcę w związku z realizacją umowy.

[akta kontroli, str. 357-364]

Umowa na wykonanie usługi diagnozy cyberbezpieczeństwa, audytu KRI, testów oprogramowaniem Rapid7 oraz szkolenie stacjonarne z zakresu cyberbezpieczeństwa, zawiera ustalenia o ochronie tajemnicy przedsiębiorstwa oraz informacji poufnych Urzędu, na rzecz którego zleceniobiorca świadczy usługi. Ponadto została zawarta umowa powierzenia przetwarzania danych osobowych, w której określono prawa i obowiązki przetwarzającego oraz administratora. Złącznikiem do przedmiotowej umowy jest informacja o kategoriach osób i danych osobowych przetwarzanych przez zleceniobiorcę.

[akta kontroli, str. 365-374]

## 10. Procedury zgłaszania incydentów naruszania BI

Podstawa prawna:

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

Katalog zagrożeń i incydentów zagrażających bezpieczeństwu danych osobowych oraz sposób reagowania na nie został opisany w Instrukcji postępowania w przypadku zagrożenia lub naruszenia ochrony danych osobowych. Dodatkowo mając na celu zapewnienie ciągłości operacyjnej oraz ograniczenie występowania przypadków naruszeń bezpieczeństwa informacji, w tym także bezpieczeństwa przetwarzania danych osobowych opracowano Procedurę zarządzania incydentami.

[akta kontroli, str. 142-143]

Z informacji uzyskanych od UM w Baborowie podczas analizy przedkontrolnej wynika, że „w ostatnich latach nie wystąpił incydent o takim charakterze”.

[akta kontroli, str. 101]

## 11. Audyt wewnętrzny z zakresu bezpieczeństwa informacji

Podstawa prawna:

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

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

Na podstawie dokumentacji przekazanej kontrolerom ustalono, że w okresie objętym kontrolą, w jednostce nie przeprowadzono obligatoryjnego audytu wewnętrznego z zakresu bezpieczeństwa informacji. Ostatni taki audyt odbył się 26 czerwca 2023 r. Ponadto dnia 29 grudnia 2023 r. w UM w Baborowie Inspektor Danych Osobowych przeprowadził audyt zgodności z RODO.

W związku z powyższym, zespół kontrolny wniósł o złożenie wyjaśnień, w których wyjaśniono, że „(...) Audyt zgodności z RODO za 2024 rok planowany jest na miesiąc grudzień 2024.

(…) Audyt KRI za 2024 rok zostanie przeprowadziny w grudniu 2024 roku, w związku z tym że przeciągnęło się postępowanie w ramach Projektu Cyberbezpieczny Samorząd. Środki uzyskano we wrześniu 2024 roku. Obecnie prowadzone jest postępowanie w celu wyłonienia wykonawcy audytu dla Urzędu na lata 2024, 2025 i 2026. Termin zakończenia postępowania ofertowego przypada na dzień 31.10.2024 r.” Załącznikami do złożonych wyjaśnień są: zapytanie ofertowe, opis przedmiotu zamówienia, formularz ofertowy oraz projekt umowy dotyczące m.in. wykonania audytów cyberbezpieczeństwa w 2024, 2025 i 2026 roku.

[akta kontroli, str. 375-431, 438-490, 497-498]

## 12. Kopie zapasowe

Podstawa prawna:

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

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

W Instrukcji zarządzania systemem informatycznym określone są wytyczne dotyczące tworzenia i przechowywania kopii zapachowych zbiorów danych osobowych, np.

- [redacted];
- [redacted];
- [redacted];
- [redacted];
- [redacted];
- [redacted].

[akta kontroli, str. 123-124]

Zgodnie z § 8 pkt 4 lit. C przedmiotowego dokumentu wszystkie kopie zapasowe są replikowane poza siedzibę Urzędu. Z wyjaśnień złożonych przez Burmistrza Gminy Baborów wynika, że [redacted]

[redacted], stwierdza się uchybienie.

[akta kontroli, str. 124, 505-506]

Dodatkowo z wyjaśnień Burmistrza Gminy Baborów wynika, że kopie zapasowe tworzone są za pomocą dedykowanego oprogramowania i sprzętu, co potwierdza dokumentacja przekazana kontrolerom.

[akta kontroli, str. 432-436, 507]

**13. Projektowanie, wdrażanie i eksploatacja systemów teleinformatycznych**

Podstawa prawna:

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

W UM w Baborowie do realizacji zadań z zakresu administracji rządowej wykorzystywane są wspomagające systemy teleinformatyczne, które dzielą się na systemy centralne, tj. CEIDG, WOW i SRP oraz system wspierający zakupiony u dostawcy zewnętrznego – WyDra (Nefeni). Na obsługę obecnie wykorzystywanego systemu informatycznego zawarta została stosowna umowa licencyjna, gwarantująca rozwój i dostosowanie do obowiązujących przepisów prawa.

[akta kontroli, str. 104-105, 357-364]

**14. Zabezpieczenia techniczno-organizacyjne dostępu do informacji**

Podstawa prawna:

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

pkt 9 - zabezpieczenie informacji w sposób uniemożliwiający nieuprawnionemu jej ujawnienie, modyfikacje, usunięcie lub zniszczenie;
pkt 11 - ustalenie zasad postępowania z informacjami, zapewniającymi minimalizację wystąpienia ryzyka kradzieży informacji i środków przetwarzania informacji, w tym urządzeń mobilnych.

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

Z dokumentacji posiadanej przez kontrolerów wynika, że w UM w Baborowie stosowane są zabezpieczenia dostępu do informacji, m.in.:

- przetwarzanie danych osobowych wyłącznie przez osoby upoważnione oraz przeszkolone;
- stosowanie zasady zachowania poufności;
- ustawianie monitorów w sposób uniemożliwiający odczytanie danych osobowych osobom nieuprawnionym;
- nie dopuszczenie do przebywania osób nieuprawnionych, w miejscach przetwarzania danych osobowych, pod nieobecność przeszkolonego pracownika;
- przechowywanie danych w sposób uniemożliwiający dostęp do nich osobom nieuprawnionym;
- tworzenie kopii zapasowych danych;
- stosowanie zapory internetowej – firewall;
- stosowanie ochrony antywirusowej;
- dostęp do danych możliwy wyłącznie poprzez zalogowanie;
- posiadanie indywidulanego loginu i hasła przez pracowników uprawnionych do przetwarzania danych.

W UM w Baborowie opracowano także Procedurę zabezpieczenia danych osobowych, która określa wytyczne oraz działania, których przestrzeganie zapewni odpowiedni poziom zabezpieczania informacji.

[akta kontroli, str. 128-130, 137-141]

W związku z wykryciem naruszeń wytycznych określonych w § 2 - Pobieranie i postępowanie z kluczami do pomieszczeń biurowych oraz § 6 - Klucze zapasowe

do pomieszczeń Procedury postępowania z kluczami, zwrócono się o złożenie wyjaśnień w przedmiotowym zakresie. Z odpowiedzi Burmistrza Gminy Baborów wynika, że [redacted]

Jednakże zespół kontrolerów nie otrzymał dokumentacji potwierdzającej wyrażenie zgody Sekretarza Gminy [redacted] Załącznikiem do złożonych wyjaśnień jest wyłącznie [redacted] Urzędu Miejskiego w Baborowie.

[akta kontroli, str. 437, 499]

Zgodnie z § 5 pkt 3 Instrukcji zarządzania systemem informatycznym oraz § 4 pkt 1 lit. c Procedury zabezpieczania danych osobowych, w pomieszczeniach, w których przetwarzane są dane osobowe, ekrany monitorów komputerowych powinny być ustawione w sposób uniemożliwiający osobom nieuprawnionym odczyt danych, a zwłaszcza nie naprzeciwko wejścia do pomieszczenia. W trakcie wizji lokalnej, zespół kontrolny ustalił, [redacted], zasada ta nie jest stosowana.

W zakresie zmiany haseł użytkowników do komputerów zapisy zawarte w pkt 9 (środki techniczne) Środki organizacyjne i techniczne niezbędne dla bezpieczeństwa danych osobowych, § 4 pkt 8 Instrukcji zarządzania systemem informatycznym oraz pkt 4 Polityki haseł są sprzeczne. [redacted]”

[akta kontroli, str. 121, 130, 188, 506]

*W związku z powyższym stwierdzono nieprawidłowości w zakresie ustawiania* ekranów monitorów w sposób umożliwiający osobom nieuprawnionym odczyt

danych, a także braku przedstawienia kontrolerom dokumentu potwierdzającego wyrażenie zgody Sekretarza Gminy [redacted]. Ponadto zostały stwierdzone uchybienia w zakresie zapisów w procedurach dot. częstotliwości zmiany haseł oraz przechowywania duplikatów kluczy do pomieszczeń Urzędu.

**15. Zabezpieczenia techniczno-organizacyjne systemów informatycznych**

Podstawa prawna:

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

W pkt 15 zostały wykazane mechanizmy jakie jednostka kontrolowana zastosowała w celu zapewnienia ochrony przetwarzanych informacji, w ramach badanych systemów teleinformatycznych przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami.

Dodatkowo zapewniono także środki uniemożliwiające nieautoryzowany dostęp oraz zapewniające kontrolę dostępu do systemów teleinformatycznych służących do realizacji zadań zleconych z zakresu administracji rządowej poprzez indywidualne logowanie do wybranych systemów, [redacted].

[akta kontroli, str. 506]

Podczas kontroli dokonano oględzin pomieszczenia serwerowni w UM w Baborowie. Czynność ta została przeprowadzona w obecności Pracownika ds. informatycznych Referatu Administracji i Ochrony Środowiska Urzędu Miejskiego w Baborowie. W toku oględzin dokonano ustalenia stanu faktycznego i stwierdzono, że:

- [redacted];
- [redacted];
- [redacted];
- [redacted];
- [redacted];
- [redacted];
- [redacted];
- [redacted];
- [redacted];
- [redacted];
- [redacted];
- [redacted];
- [redacted];
- [redacted].

Ponadto z dokumentacji przekazanej kontrolerom wynika, że:

- [redacted];
- [redacted];
- [redacted];
- [redacted];
- [redacted];
- [redacted];
- [redacted];
- [redacted];
- [redacted];
- [redacted];

[akta kontroli, str. 137-141]

W związku z udziałem UM w Baborowie w programie „Cyberbezpieczny Samorząd, zespół kontrolny poprosił o przedstawienie planu działań realizacji projektu. W odpowiedzi otrzymano dokumentację złożoną z zapytania ofertowego, opisu przedmiotu zamówienia, formularza ofertowego oraz projektu umowy

dotyczące m.in. przeprowadzenia testów penetracyjnych infrastruktury informatycznej. Dodatkową informacją przekazaną przez Burmistrza Gminy Baborów jest deklaracja o ogłoszeniu przetargu na wykonanie określonych zadań, mających na celu zapewnienie bezpieczeństwa informacji zarządzanych w UM w Baborowie.

[akta kontroli, str. 438-490, 500-501]

**16. Rozliczalność działań w systemach teleinformatycznych**

Podstawa prawna:

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

Z Procedury zabezpieczenia danych osobowych wynika, że system informatyczny i stacje robocze umożliwiają zapisywanie zdarzeń dzienników systemowych na potrzeby audytu i przechowywanie informacji o nich.[redacted].

[akta kontroli, str. 141]

Z informacji uzyskanych podczas kontroli wynika,[redacted].

Kontrolujący są w posiadaniu także dokumentu zawierającego ostatnich 100 wpisów z systemu WyDra. Natomiast w zakresie systemów CEIDG, SRP i WOW nie ma możliwości generowania logów samodzielnie. Działanie to może być wykonane jedynie poprzez współpracę z zewnętrznymi administratorami systemów. [redacted] co stanowi nieprawidłowość.

[akta kontroli, str. 102-103, 491-496, 506]

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

W wyniku kontroli stwierdzono następujące nieprawidłowości:

1. Brak opracowania, ustanowienia, wdrożenia i eksploatowania, monitorowania i przeglądania oraz utrzymania i doskonalenia Systemu Zarządzania Bezpieczeństwem Informacji, co narusza § 19 ust. 1 i 2 Rozporządzenia KRI;
2. Brak dokumentacji potwierdzającej przekazanie pracownikowi nośnika zewnętrznego;
3. Brak dokumentacji potwierdzającej przeprowadzanie inwentaryzacji oprogramowania, co narusza § 19 ust. 2 pkt 2 Rozporządzenia KRI;
4. Stosowanie Regulaminu wykonywania pracy w systemie pracy zdalnej stanowiącego załącznik do Zarządzenia w sprawie wprowadzenia Regulaminu wykonywania pracy zdalnej z nieaktualną podstawą prawną;
5. Ustawianie ekranów monitorów komputerowych w sposób umożliwiający osobom nieuprawnionym odczyt danych, co narusza § 5 pkt 3 Instrukcji zarządzania systemem informatycznym oraz § 4 pkt 1 lit. c Procedury zabezpieczania danych osobowych;
6. [redacted];
7. Brak dokumentu potwierdzającego wyrażenie zgody Sekretarza Gminy [redacted].

W wyniku kontroli stwierdzono również następujące uchybienia:

1. Zawarcie informacji w Instrukcji zarządzania systemem informatycznym [redacted];
2. Przeprowadzanie ostatniego szkolenia z zakresu ochrony danych osobowych w 2021 roku;
3. Posiadanie sprzecznych zapisów w stosowanych procedurach dotyczących częstotliwości zmiany haseł;
4. Przechowywanie duplikatów kluczy [redacted], co narusza § 6 Procedury postępowania z kluczami.

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

Kierownik jednostki kontrolowanej nie zgłosił zastrzeżeń do projektu wystąpienia pokontrolnego.

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

W związku z ustaleniami dokonanymi podczas kontroli zalecam:

1. Opracować, ustanowić, wdrożyć i eksploatować, monitorować i przeglądać, a także utrzymać i doskonalić System Zarządzania Bezpieczeństwem Informacji, zgodnie z § 19 ust. 1 i 2 Rozporządzenia KRI;
2. Przeprowadzić inwentaryzację oprogramowania służącego do przetwarzania informacji obejmującej jego rodzaj i konfigurację, zgodnie z § 19 ust. 2 pkt 2 Rozporządzenia KRI;
3. Opracować, wprowadzić oraz stosować Regulamin wykonywania pracy w systemie pracy zdalnej na aktualniej podstawie prawnej;
4. Przeprowadzić reorganizację pomieszczeń polegającą na ustawieniu ekranów monitorów komputerowych w sposób uniemożliwiający osobom nieuprawnionym odczyt danych, zgodnie z § 5 pkt. 3 Instrukcji zarządzania systemem informatycznym oraz § 4 pkt 1 lit. c Procedury zabezpieczania danych osobowych;
5. [redacted];

6. Sporządzić oraz aktualizować dokumentację potwierdzającą wyrażenie zgody Sekretarza Gminy [redacted];
7. Opracować, wprowadzić oraz stosować Instrukcję zarządzania systemem informatycznym [redacted];
8. Regularnie przeprowadzać szkolenia z zakresu ochrony danych osobowych dla wszystkich pracowników Urzędu;
9. Ujednolicić zapisy w stosowanych procedurach dotyczących częstotliwości zmiany haseł;
10. Zmienić umiejscowienie szafki, w której przechowywane są duplikaty kluczy do pomieszczeń Urzędu [redacted] zgodnie z § 6 Procedury postępowania z kluczami.

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

**VII. Na podstawie art. 49 oraz art. 46 ust. 3 pkt 3 ustawy z dnia 15 lipca 2011 r. o kontroli w administracji rządowej (t. j. Dz. U. z 2020 r. poz. 224), proszę o przekazanie pisemnej informacji o sposobie wykonania zaleceń, wykorzystaniu wniosków lub przyczynach ich niewykorzystania, o podjętych działaniach lub przyczynach ich niepodjęcia, albo o innym sposobie usunięcia stwierdzonych nieprawidłowości, w terminie 60 dni od dnia otrzymania niniejszego dokumentu.**

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

**Z up. Wojewody Opolskiego**

**Joanna Sachanbińska**
**radca prawny**
**Dyrektor**
**Wydział Prawny i Nadzoru**