WOJEWODA OPOLSKI

Opole, 22 kwietnia 2026 r.
PN.I.431.4.1.2026.AOG

Pani
Violetta Jaskólska-Palus
Burmistrz Brzegu
Urząd Miasta w Brzegu
ul. Robotnicza 12
49-300 Brzeg

WYSTĄPIENIE POKONTROLNE

I. Dane identyfikacyjne kontroli

1. Nazwa i adres jednostki kontrolowanej: Urząd Miasta w Brzegu, ul. Robotnicza 12, 49-300 Brzeg[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 2025 r. poz. 1703 ze zm.)[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 ze zm.)[3].
3. Zakres kontroli:
   a) Przedmiot kontroli: Działanie systemów teleinformatycznych i rejestrów publicznych używanych do realizacji zadań zleconych z zakresu administracji rządowej,
   b) Okres objęty kontrolą: od 1 stycznia 2025 r. do dnia rozpoczęcia kontroli

[1] UM w Brzegu
[2] Dalej: ustawa o informatyzacji działalności podmiotów
[3] Dalej: ustawa o 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: 19 lutego 2026 r. – 6 marca 2026 r., kontrola prowadzona była w trybie hybrydowym, tj. dnia 19 lutego 2026 r. – rozpoczęcie czynności kontrolnych w UM w Brzegu oraz oględziny serwerowni na miejscu w jednostce. W pozostałe dni kontrola prowadzona była zdalnie.
7. Skład zespołu kontrolnego:
   a) Agnieszka Orlińska-Gocka - Inspektor Wojewódzki w Oddziale Organizacji, Kontroli i Skarg w Wydziale Prawnym i Nadzoru w Opolskim Urzędzie Wojewódzkim – kierownik zespołu kontrolnego,
   b) Natalia Lenart - 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: Pani Violetta Jaskólska-Palus – Burmistrz Brzegu, od dnia 7 maja 2024 r.[4]
9. Kontrolę wpisano do książki kontroli prowadzonej w jednostce kontrolowanej, pod poz. nr 4/2026.

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 2025 r. do dnia rozpoczęcia kontroli (z uwzględnieniem okresu wcześniejszego i późniejszego w zakresie niezbędnym do realizacji celu kontroli), tj. 19 lutego 2026 r. w Urzędzie Miasta w Brzegu ocenia się pozytywnie z nieprawidłowościami.

W kontrolowanym okresie zakres działania i zadania oraz organizację i zasady funkcjonowania UM w Brzegu określał Regulamin Organizacyjny Urzędu Miasta

[4] Akta kontroli – Dokumenty do kontroli 1: Zaświadczenie o wyborze Burmistrza; Dokumenty do kontroli 2: Ślubowanie Burmistrza;

w Brzegu[5] stanowiący załącznik do Zarządzenia nr 1054/2025 Burmistrza Brzegu z dnia 27 maja 2025 r. w sprawie nadania Regulaminu Organizacyjnego Urzędu Miasta w Brzegu, aktualizowany zarządzeniem nr 1149/2025 Burmistrza Brzegu z dnia 11 lipca 2025 r. ws. zmian do Regulaminu Organizacyjnego Urzędu Miasta w Brzegu[6].

Zgodnie z § 2 pkt 1 Regulaminu organizacyjnego pracą Urzędu kieruje Burmistrz na zasadzie jednoosobowego kierownictwa.

Osobami pełniącymi funkcję Administratorów Systemów Informatycznych[7] są: Główny Specjalista ds. Informatyki oraz Informatyk, będący pracownikami UM w Brzegu.[8] Osoby te są jednocześnie odpowiedzialne za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa. Zgłoszenie osób do CSIRT NASK nastąpiło dnia 17 października 2019 roku.[9]

W UM w Brzegu do realizacji zadań zleconych z zakresu administracji rządowej wykorzystywanych jest 5 systemów teleinformatycznych[10], w tym:

- 2 o zasięgu krajowym;
- 3 o zasięgu lokalnym.

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.

Na stronie głównej Biuletynu Informacji Publicznej UM w Brzegu została udostępniona Elektroniczna Skrzynka Podawcza: /umbrzeg/skrytka, znajdująca się na Elektronicznej Platformie Usług Administracji Publicznej, pozwalająca na wysyłanie i odbieranie pism w formie dokumentów elektronicznych. Dodatkowo na BIP został udostępniony adres do doręczeń elektronicznych, tj. AE:PL-33308-16783-FFRWV-34, który UM w Brzegu posiada zgodnie z art. 8 ustawy z dnia 18 listopada 2020 r. o doręczeniach elektronicznych (t.j. Dz.U. z 2026 r. poz. 3).

[5] Dalej: Regulamin organizacyjny
[6] Akta kontroli –Dokumenty do kontroli 1: Regulamin Organizacyjny Urzędu Miasta w Brzegu, Zmiany w Regulaminie Organizacyjnym Urzędu Miasta w Brzegu
[7] Dalej: ASI
[8] Akta kontroli – Dokumenty do kontroli 1: Zakres czynności - A.H., Zarządzenie ASI,
[9] Akta kontroli – Dokumenty do kontroli 1: Zarządzenie CSIRT
[10] Akta kontroli - Dokumentacja kontrolna 1: Załącznik nr 1 - Zestawienie systemów teleinformatycznych

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[11]: Zarządzanie bezpieczeństwem informacji 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.

Z informacji uzyskanych w analizie przedkontrolnej wynika, że w UM w Brzegu podstawowym sposobem dokumentowania przebiegu załatwiania i rozstrzygania spraw jest elektroniczny system wykonywania czynności kancelaryjnych (EZD – system Elektronicznego Zarządzania Dokumentacją)[12].

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;

[11] Dz.U. z 2024 r. poz. 773, dalej: Rozporządzenie KRI
[12] Akta kontroli - § 23 ust. 2 pkt 1i Regulaminu Organizacyjnego.

- § 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[13], 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.

Podstawowym elementem SZBI jest Polityka Bezpieczeństwa Informacji[14], 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.

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 Brzegu został opracowany i ustanowiony, wdrożony i eksploatowany, monitorowany i przeglądany oraz utrzymywany i doskonalony System Zarządzania Bezpieczeństwem Informacji, który został wprowadzony zarządzeniem nr 1558/2020 Burmistrza Brzegu z dnia 3 listopada 2020 r. w sprawie wprowadzenia „Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie Miasta w Brzegu” oraz „Polityki bezpieczeństwa w zakresie przetwarzania danych w tym danych osobowych w Urzędzie Miasta w Brzegu” oraz zmieniony Zarządzeniem Nr 98/2024 Burmistrza Brzegu z dnia 10 czerwca 2024 r. w sprawie zmiany Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie Miasta w Brzegu” oraz „Polityki bezpieczeństwa w zakresie przetwarzania danych w tym danych osobowych w Urzędzie Miasta w Brzegu”.

[13] Dalej: SZBI
[14] Dalej: PBI

Z dokumentacji przekazanej kontrolerom wynika, że na SZBI składają się Polityka Bezpieczeństwa w zakresie przetwarzania danych w tym danych osobowych oraz Instrukcja Zarządzania Systemem Teleinformatycznym wraz z politykami towarzyszącymi i inni dokumentami, m.in. Regulaminem Korzystania z Zasobów Informatycznych, Procedurą Zarządzania Incydentami Cyberbezpieczeństwa oraz Polityką Ochrony Danych Osobowych.[15] Podmiot nie przedstawił dokumentacji potwierdzającej zapoznanie się z aktualnie obowiązującym SZBI przez pracowników UM w Brzegu, co zespół kontrolny uznaje za nieprawidłowość.

Z Raportu Systemu Zarządzania Bezpieczeństwem Informacji wynika, że ostatni przegląd SZBI odbył się w grudniu 2025 r.[16] UM w Brzegu aktualnie znajduje się na etapie projektowania nowej dokumentacji SZBI w ramach projektu „Cyberbezpieczny Samorząd". Znajduje się ona na etapie wdrażania, więc na chwilę obecną brak jest dokumentacji potwierdzającej zapoznanie się z nią przez pracowników UM w Brzegu[17].

W UM w Brzegu został wyznaczony Pełnomocnik ds. bezpieczeństwa informacji, który jednocześnie pełni funkcję Inspektora Ochrony Danych Osobowych.[18] Zgodnie z art. 38 ust. 6 RODO – IOD może wykonywać inne zadania i obowiązki po warunkiem, że nie powodują one konfliktu interesów. W przypadku połączenia funkcji IOD z zadaniami związanymi z nadzorem lub bezpośrednim zarządzaniem systemem bezpieczeństwa informacji istnieje ryzyko, że powołana na te stanowiska osoba będzie zobowiązana do monitorowania i oceniania procesów, za których realizację sama odpowiada. Może to podważyć niezależność i bezstronność IOD, co jest kluczowe dla skutecznego wykonywania tej funkcji. W związku z powyższym zasadnym jest przeprowadzenie precyzyjnej, udokumentowanej analizy ryzyka co do ewentualnego konfliktu interesów w obecnym modelu organizacyjnym. Analiza ta powinna obejmować szczegółowy zakres obowiązków przypisanych IOD oraz ocenę ich potencjalnego wpływu na zdolność do niezależnego sprawowania nadzoru nad przetwarzaniem danych osobowych.

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

[15] Akta kontroli – Dokumenty do kontroli 1: Zarządzenie Nr 98/2024 Burmistrza Brzegu
[16] Akta kontroli – Dokumenty do kontroli 2: Raport audytu SZBI
[17] Akta kontroli – Dokumenty do kontroli 2: Wyjaśnienia UM w Brzegu
[18] Dalej: IOD

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 przeciwdziałanie zagrożeniom, ograniczenie skutków zmaterializowanych ryzyk oraz 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 przesłanej dokumentacji wynika, że w 2025 r. w UM w Brzegu została przeprowadzona analiza ryzyka z zakresu bezpieczeństwa informacji.[19]

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 o nich. Stworzona baza ma na celu podejmowanie właściwych decyzji i działań w zakresie zmian w środowisku teleinformatycznym.

W UM w Brzegu prowadzone są zestawienia sprzętu komputerowego, informatycznego oraz oprogramowania informatycznego, które zapewniają

[19] Akta kontroli – Dokumenty do kontroli 2: Ewidencja ryzyka 2025

utrzymanie aktualności użytkowanego sprzętu i oprogramowania. Przedmiotowa inwentaryzacja odbywa się w systemie e-Audytor [20].

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.

Pracownicy UM w Brzegu realizujący zadania zlecone z zakresu administracji rządowej posiadają upoważnienia do przetwarzania informacji wraz z odpowiednimi uprawnieniami w systemach, które zgodne są z ich zakresami czynności.

Proces nadania/zmiany/cofania uprawnień dostępu do systemów odbywa się poprzez złożenie wniosku za pośrednictwem systemu EZD do IOD, a następnie nadanie, zmianę lub odebranie uprawnień przez Administratora Systemu Teleinformatycznego.[21]

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

[20] zgodnie z § 4 ust. 7 pkt 2 Instrukcji zarządzania systemem teleinformatycznym w UM w Brzegu, będącej częścią dokumentacji SZBI; Dokumenty do kontroli 2: Metryka komputera
[21] zgodnie z § 3 ust. 1-4 Instrukcji zarządzania systemem teleinformatycznym w UM w Brzegu, będącej częścią dokumentacji SZBI.

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 BI oraz zabezpieczenia przed takimi incydentami, szkolenia osób zaangażowanych w proces przetwarzania informacji powinny być przeprowadzane cyklicznie.

W 2025 r. w UM w Brzegu zostały przeprowadzone szkolenia zewnętrzne z zakresu bezpieczeństwa informacji oraz RODO (dla kadry kierowniczej).

Zgodnie z zapisami Polityki bezpieczeństwa w zakresie przetwarzania danych w tym danych osobowych w UM w Brzegu (rozdział III ust. 4 pkt. 2) systematyczne kształcenie pracowników z zakresu aktualnych zagrożeń bezpieczeństwa jest realizowane co najmniej raz w roku.

Szkolenie z zakresu informacji o zagrożeniach cyberbezpieczeństwa, na podstawie rozdziału VIII ust. 1, 3 i 6 Procedury Zarządzania Incydentami Bezpieczeństwa[22], przeprowadza corocznie zespół KSC składający się m.in. z IOD oraz ASI. Każde szkolenie wewnętrzne powinno być udokumentowane poprzez sporządzenie dokumentu potwierdzającego uczestnictwo w takim szkoleniu przez jego uczestników (lista obecności).

W związku z powyższym, brak przeprowadzenia szkolenia wewnętrznego z zakresu bezpieczeństwa oraz RODO dla wszystkich pracowników, zespół kontrolny stwierdza jako nieprawidłowość.

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.

[22] Załącznik nr 7 do Instrukcji Zarządzania Systemem Teleinformatycznym, będącej częścią dokumentacji SZBI

W UM w Brzegu zostały ustanowione podstawowe zasady gwarantujące bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość określone w Regulaminie Pracy Zdalnej w Urzędzie Miasta w Brzegu stanowiącym załącznik do Zarządzenia nr 4131/2023 Burmistrza Brzegu z dnia 21 lipca 2023 r. w sprawie ustalenia Regulaminu Pracy Zdalnej w UM w Brzegu[23]. W okresie objętym kontrolą miały miejsce przypadki przechodzenia pracowników na pracę zdalną. Z przesłanej dokumentacji wynika, że w UM w Brzegu jest prowadzony rejestr pracy zdalnej[24].

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.

W UM w Brzegu wykorzystywane są dwa systemy teleinformatyczne przeznaczone do realizacji zadań zaleconych z zakresu administracji rządowej zakupione u zewnętrznego dostawcy. W związku z tym zostały podpisane stosowne umowy licencyjne umożliwiające prawidłową eksploatację. Do jednej z umów nie dołączono umowy powierzenia przetwarzania danych osobowych, co UM w Brzegu uzasadnił w przesłanych wyjaśnieniach: „ Firma Sygnity nie zawiera umów powierzenia, gdyż nie ma dostępu do danych. Aktualizacje przeprowadza samodzielnie informatyk urzędu. Firma Sygnity zawiera umowy powierzenia w momencie przesłania danych do serwisu. Nie było konieczności przesyłania bazy do serwisu, tym samym nie było potrzeby zawierania umowy powierzenia danych”[25]. Zespół kontrolny przyjął powyższe wyjaśnienia.

10. Procedury zgłaszania incydentów naruszania BI

Podstawa prawna:

[23] Akta kontroli – Zarządzenie Nr 4131/2023 Burmistrza Brzegu z dnia 21 lipca 2023 roku ws. ustalenia Regulaminu Pracy Zdalnej w UM w Brzegu
[24] Akta kontroli – Dokumenty do kontroli 2: Rejestr pracy zdalnej
[25] Akta kontroli – Dokumenty do kontroli 2: Wyjaśnienia UM w Brzegu

- § 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.

W Procedurze Zarządzania Incydentami Cyberbezpieczeństwa zostały określone wytyczne oraz sposób postępowania ze zdarzeniami związanymi z naruszeniem bezpieczeństwa informacji, które mają na celu zapewnienie ciągłości operacyjnej oraz ograniczenie występowania takich incydentów w przyszłości. Dodatkowo zostały sporządzone dokumenty ułatwiające nadzór nad występującymi incydentami, tj. Raport naruszenia/incydentu bezpieczeństwa oraz Rejestr incydentów cyberbezpieczeństwa[26].

Z informacji uzyskanych z UM w Brzegu wynika, że w okresie objętym kontrolą nie miały miejsca przypadki wystąpienia incydentów naruszenia bezpieczeństwa informacji.[27]

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 SZBI jednostki z kryteriami audytu.

Z dokumentacji przekazanej kontrolerom wynika, że ostatni audyt przeprowadzony przez firmę zewnętrzną odbył się w 2024 roku[28]. W trakcie kontroli ustalono, że w okresie objętym kontrolą, w jednostce nie przeprowadzono obligatoryjnego audytu wewnętrznego z zakresu bezpieczeństwa informacji, co zespół kontrolny stwierdza jako nieprawidłowość.

12. Kopie zapasowe

[26] Akta kontroli: Dokumenty do kontroli 1: Procedura Zarządzania Incydentami Cyberbezpieczeństwa, będąca częścią dokumentacji SZBI
[27] Akta kontroli – Dokumenty do kontroli 2: Rejestr incydentów.
[28] Akta kontroli – Dokumenty do kontroli 1: Audyt – analiza zgodności bezpieczeństwa informacji

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 celu zapewnienia bezpieczeństwa informacji oraz systemów teleinformatycznych, w których informacje te są przetwarzane, UM w Brzegu sporządził procedury tworzenia kopii zapasowych określone w § 4 pkt 8 Instrukcji Zarządzania Systemem Teleinformatycznym w UM w Brzegu, obejmujące m.in. harmonogram tworzenia kopii, sposób przechowywania, nadzór nad procesem ich wykonywania.[29]

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 Brzegu do realizacji zadań z zakresu administracji rządowej wykorzystywane są wspomagające systemy teleinformatyczne, które dzielą się na systemy centralne oraz lokalne (zakupione u dostawcy zewnętrznego).
Na obsługę zakupionych systemów informatycznych zawarte zostały stosowne umowy licencyjne, gwarantujące rozwój i dostosowanie do obowiązujących przepisów prawa. Przedmiotowe systemy teleinformatyczne zostały zaprojektowane,

[29] będącej częścią dokumentacji SZBI.

wdrożone i eksploatowane z uwzględnieniem ich funkcjonalności, niezawodności, używalności, wydajności, przenoszalności i pielęgnowalności.

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 bezpieczeństwa informacji 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 kontrolowanej dokumentacji wynika, że w UM w Brzegu stosowane są zabezpieczenia dostępu do informacji, które zostały określone m.in. w Polityce Bezpieczeństwa w zakresie przetwarzania danych w tym danych osobowych[30].

W UM w Brzegu pomieszczenia, w których przetwarzane są dane osobowe, zabezpieczone są przed dostępem do nich osób nie posiadających uprawnień do przetwarzania danych osobowych. Osoby nie posiadające takich uprawnień mogą przebywać w nich jedynie w obecności osób uprawnionych. Sprawowany jest również właściwy nadzór nad kluczami do pomieszczeń oraz kontrola dostępu wraz z rejestracją wejść i wyjść do głównej serwerowni.

[30] Akta kontroli – Dokumenty do kontroli 1: Załącznik Nr 6 do Polityki Bezpieczeństwa w zakresie przetwarzania danych w tym danych osobowych, będącej częścią SZBI - Środki techniczne i organizacyjne stosowane przez Administratora w celu zapewnienia poufności, integralności i rozliczalności przy przetwarzaniu danych.

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.

Poza zabezpieczeniami techniczno-organizacyjnymi dostępu do informacji, w Polityce Bezpieczeństwa w zakresie przetwarzania danych w tym danych osobowych zostały określone także zabezpieczenia dla systemów informatycznych.

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[31].

Podczas kontroli dokonano oględzin dwóch pomieszczeń stanowiących serwerownie w UM w Brzegu. Czynność ta została przeprowadzona w obecności IOD[32]. Zespół kontrolny rekomenduje, aby do serwerowni monitoringu było tylko jedno wejście ze wzmocnionymi drzwiami, z kontrolą dostępu i rejestracją wejść i wyjść. Zespół kontrolny zaleca jednocześnie w obu serwerowniach monitoring wewnętrzny, czujniki m.in. dymu, zawilgocenia i temperatury, ewentualny czujnik otwarcia szafy sieciowej, celem podniesienia poziomu bezpieczeństwa przetwarzanych danych.

16. Rozliczalność działań w systemach teleinformatycznych

Podstawa prawna:

[31] Akta kontroli – Dokumenty do kontroli 2: Wyjaśnienia UM w Brzegu.
[32] Akta kontroli - Protokół oględzin

- § 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 dokumentacji oraz informacji uzyskanych w trakcie kontroli wynika, że UM w Brzegu odnotowuje obligatoryjne działania użytkowników w dziennikach systemów, które są przechowywane przez okres 2 lat, w zależności od posiadanego sprzętu.[33]

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

W wyniku kontroli stwierdzono następujące nieprawidłowości:

1. Brak potwierdzenia zapoznania się z aktualnie obowiązującym SZBI przez pracowników UM w Brzegu;
2. Brak przeprowadzenia audytu z zakresu bezpieczeństwa informacji, co narusza § 19 ust. 2 pkt 14 rozporządzenia KRI;
3. Brak przeprowadzenia szkolenia wewnętrznego z zakresu bezpieczeństwa oraz RODO dla wszystkich pracowników UM w Brzegu.

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

[33] § 4 ust. 6 pkt 3f Instrukcji Zarządzania Systemem Teleinformatycznym w UM w Brzegu, będącej częścią SZBI.

Nie zgłoszono 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. Dokumentować fakt zapoznania się z aktualnie obowiązującym SZBI przez pracowników UM w Brzegu;
2. Przeprowadzać audyty z zakresu bezpieczeństwa informacji;
3. Przeprowadzać szkolenia wewnętrzne z zakresu bezpieczeństwa oraz RODO dla wszystkich pracowników UM w Brzegu.

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 30 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
Dyrektor
Wydział Prawny i Nadzoru

Pismo zostało wydane w postaci elektronicznej i podpisane kwalifikowanym podpisem elektronicznym.