WOJEWODA DOLNOŚLĄSKI

Wrocław, dnia 19 września 2023 r.

NK-KSE.431.2.4.2023.WK

Pan
Daniel Gibski
Dolnośląski Wojewódzki Konserwator Zabytków

WYSTĄPIENIE POKONTROLNE

Na podstawie art. 6 ust. 4 pkt 1 ustawy z dnia 15 lipca 2011 r. o kontroli w administracji rządowej[1], art. 28 ust. 1 pkt 1 ustawy z dnia 23 stycznia 2009 r. o wojewodzie i administracji rządowej w województwie[2], a także imiennych upoważnień do przeprowadzenia kontroli nr: NK-KSE.0030.59.2023.WK, NK-KSE.0030.60.2023.WK, NK-KSE.0030.61.2023.WK, NK- KSE.0030.62.2023.WK oraz NK-KSE.0030.63.2023.WK udzielonych przez Wojewodę Dolnośląskiego w dniu 23 maja 2023 r., zespół kontrolujący w składzie: Weronika Kornacka – inspektor wojewódzki z Wydziału Prawnego, Nadzoru i Kontroli (przewodniczący zespołu kontrolnego), Aleksandra Grzebieniowska – inspektor wojewódzki z Wydziału Prawnego, Nadzoru i Kontroli (członek zespołu kontrolnego), Tomasz Woch – starszy inspektor wojewódzki z Wydziału Prawnego, Nadzoru i Kontroli (członek zespołu kontrolnego) Anna Adamowska – Kierownik Oddziału Sieci i Systemów Informatycznych z Biura Administracji i Logistyki (członek zespołu kontrolnego) oraz Tadeusz Daleczko – starszy informatyk z Biura Administracji i Logistyki (członek zespołu kontrolnego), w dniach od 25 maja 2023 r. do 30 czerwca 2023 r. przeprowadził kontrolę problemową w trybie zwykłym w Wojewódzkim Urzędzie Ochrony Zabytków we Wrocławiu (dalej jako: „jednostka kontrolowana" lub „WUOZ") z siedzibą przy ul. Władysława Łokietka 11, 50-243.

Kontrola została zrealizowana zgodnie z zatwierdzonym w dniu 22 grudnia 2022 r. przez Wojewodę Dolnośląskiego planem kontroli na I półrocze 2023 r. nr NK-KSE.430.7.2022.TW.

Tematyka kontroli obejmowała Bezpieczeństwo teleinformatyczne jednostki - działanie systemów teleinformatycznych oraz rejestrów publicznych używanych do realizacji zadań administracji rządowej na podstawie przepisów ustawy z dnia 17 lutego 2005 r.

[1] t.j. Dz. U. z 2020 r. poz. 224.
[2] t.j. Dz.U. z 2023 r. poz. 190.

o informatyzacji działalności podmiotów realizujących zadania publiczne[3] oraz rozporządzenia z dnia 12 kwietnia 2012 r. Rady Ministrów w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych[4] – w okresie od dnia 1 stycznia 2020 r. do dnia kontroli.

Celem kontroli była ocena działalności jednostki kontrolowanej w zakresie tematyki objętej kontrolą, dokonana na podstawie ustalonego stanu faktycznego przy zastosowaniu przyjętych kryteriów kontroli, a w przypadku stwierdzenia nieprawidłowości ustalenie ich zakresu, przyczyn i skutków oraz osób za nie odpowiedzialnych, a także sformułowanie zaleceń pokontrolnych zmierzających do usunięcia nieprawidłowości.

Ocena działalności jednostki kontrolowanej w zakresie objętym kontrolą została dokonana na podstawie ustalonego stanu faktycznego, w oparciu o udostępnione w toku wykonywania czynności kontrolnych dokumenty oraz złożone wyjaśnienia kontrolowanego pismami z dnia 6 czerwca 2023 r., 12 czerwca 2023 r. i 23 czerwca 2023 r. przy zastosowaniu kryteriów kontroli wynikających z ustawy o kontroli w administracji rządowej, tj. legalności oraz rzetelności.
[dowód: akta kontroli str. 100-137]

W okresie objętym kontrolą funkcję Dolnośląskiego Wojewódzkiego Konserwatora Zabytków pełnili:
- Pani Barbara Nowak-Obelinda – do 12 sierpnia 2021 r.,
- Pan Daniel Gibski – od 12 października 2021 r. – obecnie.

[dowód: akta kontroli str.105-106]

Bezpieczeństwo teleinformatyczne jednostki - działanie systemów teleinformatycznych oraz rejestrów publicznych używanych do realizacji zadań administracji rządowej oceniono ***pozytywnie z nieprawidłowościami.***

Powyższą ocenę uzasadniają następujące ustalenia z kontroli.

Pismem nr NK-KSE.431.2.4 2023.WK z dnia 20 lipca 2023 r. przekazano kierownikowi jednostki kontrolowanej projekt wystąpienia pokontrolnego, do którego we wskazanym terminie wniesiono zastrzeżenia. Zastrzeżenie dot. ustalenia zawartego w części C pkt 3 projektu wystąpienia pokontrolnego uwzględniono, zaś w pozostałym zakresie wniesione zastrzeżenia oddalono.

W związku z powyższym, zgodnie z dyspozycją art. 46 ust. 2 w zw. z art. 47 ustawy o kontroli w administracji rządowej, przekazuję niniejsze wystąpienie pokontrolne.

---

[3] t.j. Dz.U. z 2023 r. poz. 57, zwanej dalej: „ustawą o informatyzacji".
[4] t.j. Dz. U. z 2017 r. poz. 2247, zwanym dalej: r.k.r.i.

A. Świadczenie usług drogą elektroniczną.

Do jednych z podstawowych celów funkcjonowania urzędu zalicza się realizowanie usług w sposób szybki, sprawny i możliwie jak najbardziej przyjazny dla obsługiwanego podmiotu. Realizację powyższych postulatów w praktyce można uzyskać świadcząc te usługi poprzez platformę elektroniczną dostępną za pośrednictwem sieci Internet. Taki sposób realizacji umożliwia załatwianie spraw w urzędzie bez wychodzenia z domu lub z dowolnego innego miejsca, w którym klient ma dostęp do Internetu. Ma to na celu ułatwienie, jak i usprawnienie obsługi podmiotów, a także eliminowanie korespondencji papierowej na rzecz elektronicznych formularzy i dokumentacji, wypełnianych na platformie usług elektronicznych organu.

Zgodnie z art. 16 ust. 1a ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne[5] podmiot publiczny udostępnia elektroniczną skrzynkę podawczą, spełniającą standardy określone i opublikowane na ePUAP przez ministra właściwego do spraw informatyzacji, oraz zapewnia jej obsługę. W wyniku kontroli ustalono, iż podmiot kontrolowany na stronie podmiotowej Biuletynu Informacji Publicznej pod adresem http://wosoz.ibip.wroc.pl/public/ zamieścił wymaganą informację o dostępnym adresie Elektronicznej Skrzynki Podawczej: /dwkz/skrytka. Niemniej jednak, adres ten nie został zamieszczony prawidłowo – w formie identyfikatora URI, co narusza obowiązek wynikający z § 3 ust. 1 pkt 1 Rozporządzenia Prezesa Rady Ministrów z dnia 14 września 2011 r. w sprawie sporządzania i doręczania dokumentów elektronicznych oraz udostępniania formularzy, wzorów i kopii dokumentów elektronicznych[6]. Kontrolowany organ wyjaśnił, iż:

> *„WUOZ nie umieszcza na stronie przedmiotowej BIP adresu skrzynki podawczej (ESP) w formie identyfikatora URI, ponieważ jeszcze usługa ta nie została wprowadzona ze względu na ograniczone środki Urzędu. Trwają prace nad rozwiązaniem tego problemu".*

[dowód: akta kontroli str. 104]

Wyjaśnienie uznane zostało za przyczynę powyższej nieprawidłowości.

W toku kontroli prowadzono skuteczną korespondencję z jednostką kontrolowaną za pośrednictwem platformy ePUAP, tym samym stwierdzono, że WUOZ we Wrocławiu zapewnia możliwość świadczenia elektronicznych usług na rzecz obywateli/klientów.

[dowód: akta kontroli str. 1-33, 100-137]

W toku czynności kontrolnych ustalono, iż WUOZ udostępnia na stronie podmiotowej BIP pod adresem http://wosoz.ibip.wroc.pl/public/?id=2534 informacje o świadczeniu usług (o sposobie składania dokumentów), nazwie usługi, podstawie prawnej, procedurze załatwienia sprawy. Na stronie udostępniono również wzory wniosków w formie edytowalnej. Stwierdzono natomiast, iż brak jest informacji o wymaganiach określonych przepisami prawa dotyczących doręczania dokumentów elektronicznych. Kontrolowany organ wyjaśnił, iż:

> *„Nie zamieszczono informacji o warunkach doręczania do podmiotu dokumentów elektronicznych. Rok 2022 był szczególnie trudny dla funkcjonowania jednostki, wypowiedzenie porozumienia dotyczącego Miejskiego Konserwatora Zabytków i reorganizacja urzędu wymusiła*

[5] Tekst jedn. Dz. U. z 2023 r. poz. 57.

[6] Tekst jedn. Dz.U. z 2018, poz.180, zwane dalej: r.s.d.u.

wykonanie w pierwszej kolejności innych zadań. Jesteśmy w trakcie opracowywania i wdrożenia na stronie BIP przedmiotowej treści."

[dowód: akta kontroli str. 70, 134, 136]

Wyjaśnienia uznano za przyczynę niezrealizowania obowiązku. Wskazać wymaga, iż powyższe nie jest zgodne z § 3 ust. 1 r.s.d.u.

Korespondencja w toku kontroli z jednostką kontrolowaną wykazała, że Elektroniczna Skrzynka Podawcza działająca w ramach platformy ePUAP jednostki kontrolowanej realizuje obowiązek automatycznego generowania poświadczenia przedłożenia, zgodnie z obowiązkiem wynikającym z § 13 r.s.d.u.

[dowód: akta kontroli str. 138]

W wyniku kontroli ustalono, że Elektroniczna Skrzynka Podawcza działająca w ramach platformy ePUAP jednostki kontrolowanej udostępnia adresatowi dokumentu elektronicznego poświadczenie doręczenia w celu umożliwienia podpisania poświadczenia doręczenia, zgodnie z § 14 - § 16 r.s.d.u.

[dowód: akta kontroli str. 109]

W wyniku kontroli ustalono także, iż system teleinformatyczny służący do obsługi doręczeń w jednostce podlegającej kontroli zapewnia oznaczanie doręczonych dokumentów elektronicznych danymi stwierdzającymi ważność podpisów elektronicznych w momencie ich złożenia i czas ich weryfikacji, co jest zgodne z § 5 r.s.d.u.

[dowód: akta kontroli str.110]

Mając na uwadze powyższe ustalenia, wskazany obszar należy ocenić ***pozytywnie z nieprawidłowościami.***

B. Współpraca systemów teleinformatycznych z innymi systemami (interoperacyjność).

Realizując czynności kontrolne analizie poddano dwa użytkowane w WUOZ systemy teleinformatyczne z przekazanego w piśmie w dniu 19 maja 2023 r. „zestawienia systemów teleinformatycznych używanych do realizacji zadań zleconych" tj. program Progman (poz. nr 12 zestawienia) oraz program e-dok (poz. nr 9 zestawienia).

Zgodnie z przekazanymi informacjami w ww. zestawieniu, system Progman przetwarza dane księgowe i kadrowo-płacowe, jest systemem lokalnym, nie posiada redundancji.

Z kolei w przypadku systemu e-dok wskazano, że jest to system lokalny zapewniający dostęp z wszystkich delegatur i użytkowników pracujących przez kanały VPN, nie posiada dostępu publicznego. System działa w środowisku wirtualnym i posiada redundancję.

Dodatkowo, w piśmie z 12 czerwca 2023 WUOZ.1610.1.2023.DG kontrolowany przekazał informacje na temat sposobu w jaki systemy Progman i eDOK przekazują dane do innych systemów:

„Oprogramowanie Progman przekazuje dane do systemu Płatnik używając formatu XML i standardu kodowania znaków UTF-8, załącznik nr 5 udowadnia opisaną funkcjonalność. Pisma wychodzące z programu eDOK do ePUAP przekazywane są za pomocą formatu XML, PDF oraz xAdES, załącznik nr 6 przedstawia tą funkcjonalność."

[dowód: akta kontroli str. 120]

Czynności kontrolne wykazały, że Progman jest systemem lokalnym, służącym zarządzaniu danymi księgowymi i kadrowo-płacowymi. Progman umożliwia wymianę danych z innymi systemami - eksportuje dane do zewnętrznych systemów: systemu Płatnik - za pomocą pliku w formacie XML, ze stroną kodową UTF-8.

Jak stanowi § 18 ust. 1 r.k.r.i. *„systemy teleinformatyczne podmiotów realizujących zadania publiczne udostępniają zasoby informacyjne co najmniej w jednym formatów danych określonych w załączniku nr 2 do rozporządzenia"*. Jednym z formatów danych jest format .XML (Extensible Markup Language).

Program e-dok jest systemem obiegu dokumentów. Program e-dok jest zintegrowany z platformą ePUAP, która to pozwala na wymianę dokumentów pomiędzy instytucjami i obywatelami.

Programy Progman oraz e-dok przesyłają dane do zewnętrznych programów przez co spełniają wymogi interoperacyjności.

Wobec powyższego stwierdzono, iż użytkowane w WUOZ programy spełniają wymagania § 17 ust. 1 oraz 18 ust. 1 i 2 rozporządzenia KRI, zagadnienie zostało zatem ocenione **pozytywnie.**

C. System zarządzania bezpieczeństwem informacji w systemach teleinformatycznych.

1. Dokumenty z zakresu systemu bezpieczeństwa informacji.

Mając na uwadze przepis § 20 ust. 1 r.k.r.i, podmiot realizujący zadania publiczne zobowiązany jest do opracowania i ustanowienia, wdrożenia i eksploatowania, monitorowania i przeglądania, a także utrzymywania i doskonalenia systemu zarządzania bezpieczeństwem informacji, zwany dalej SZBI, zapewniającego poufność, dostępność oraz integralność informacji z uwzględnieniem takich atrybutów, jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność. Niezbędne jest więc opracowanie kompleksowej dokumentacji SZBI, w tym również odpowiednich regulacji wewnętrznych, a także zapewnienie ich aktualizacji w zakresie dot. zmieniającego się otoczenia. Dokumentacja musi być sporządzona w sposób precyzyjny, nie może pozostawiać wątpliwości co do stosowania zawartych w niej reguł, ponieważ dotyczy wszystkich użytkowników mających dostęp oraz przetwarzających informacje. Opracowanie wszechstronnej dokumentacji SZBI umożliwia efektywne wykonywanie zadań w jednostce, a także właściwe zarządzanie bezpieczeństwem informacji oraz zabezpieczenie interesów jednostki. Kompleksowe podejście do omawianej tematyki powinno uwzględniać rozmaite kategorie informacji, odnosząc się do ich zabezpieczenia, z uwzględnieniem właściwej klasyfikacji, zależnej od profilu działalności podmiotu, m.in. bezpieczeństwo osobowe, informatyczne, fizyczne, prawne, czy technologie oraz tajemnice jednostki. Jednym z najważniejszych elementów, wchodzących w zakres dokumentacji SZBI jest Polityka Bezpieczeństwa Informacji, która powinna zostać zatwierdzona przez kierownictwo podmiotu, przekazana pracownikom do zapoznania, a następnie regularnie poddawana przeglądowi. Doskonalenie całego SZBI jest szczególnie istotne, ponieważ zapewnia aktualność wszystkich regulacji, co znacząco wpływa na zagwarantowanie właściwego poziomu bezpieczeństwa.

W ankiecie dotyczącej działania systemów teleinformatycznych kontrolowana jednostka wskazała, iż nie opracowano, ani nie wdrożono SZBI. Niemniej jednak w toku

przeprowadzonej kontroli ustalono, iż w dniu 29 stycznia 2021 r. zostało wydane zarządzenie nr 6 w sprawie wdrożenia procedur Ochrony Danych Osobowych (...) (dalej jako: Zarządzenie z 2021 r.). Jego przepisy zakładają, iż każdy pracownik WUOZ ma obowiązek zapoznać się z jego treścią oraz odbyć szkolenie w zakresie stosowania powyższych przepisów. Załącznikami do Zarządzenia z 2021 r. są m.in.: Instrukcja Zarządzania Systemem Informatycznym, Instrukcja Naruszeń i Regulamin Pracy Zdalnej. Ponadto w czasie kontroli stwierdzono, iż w dniu 3 grudnia 2019 r. zostało wydane Zarządzenie nr 39/2019 w sprawie wprowadzenia polityki bezpieczeństwa informacji i systemów teleinformatycznych w WUOZ we Wrocławiu wraz z polityką haseł (dalej jako: Zarządzenie z 2019 r.). Wszystkie wskazane dokumenty zostały formalnie zatwierdzone przez kierownictwo jednostki.

Analiza zapisów Zarządzenia z 2019 r. wykazała, iż zawiera ono:

- minimalne wymogi dotyczące bezpieczeństwa logicznego oraz fizycznego dla systemów informatycznych stosowanych w WUOZ oraz przetwarzanych w nich danych,
- wymagania w zakresie zapewnienia bezpieczeństwa pomieszczenia serwerowni i infrastruktury teleinformatycznej w niej zlokalizowanej,
- wytyczne mające zapewnić bezpieczeństwo danych przetwarzanych w WUOZ (m. in. w zakresie upoważnień w dostępie do danych ograniczonym zakresem obowiązków, wytyczne w zakresie wykonywania kopii zapasowych oraz stosowanego oprogramowania),
- zasady klasyfikacji danych przetwarzanych w kontrolowanej jednostce,
- zasady zapewnienia bezpieczeństwa danych powierzonych podmiotom zewnętrznych na podstawie zawartych z nimi umów,
- politykę haseł obowiązującą w WUOZ.

[dowód: akta kontroli str.: 72-88]

Mając na uwadze powyższe należy stwierdzić, iż obowiązujące w jednostce kontrolowanej dokumenty odnoszą się zarówno do bezpieczeństwa informacji jak i do bezpieczeństwa danych osobowych. Niemniej jednak, widocznym jest, iż temat bezpieczeństwa danych osobowych został uregulowany w bardziej dokładny i rozbudowany sposób niż temat bezpieczeństwa danych. Dane osobowe są bardzo istotnym, ale tylko jednym z wielu obszarów informacji, które należy odpowiednio zabezpieczać i chronić. Pojęcie bezpieczeństwa informacji jest pojęciem szerszym, obejmującym różne kategorie informacji. Dlatego też należy negatywnie ocenić fakt, iż polityka bezpieczeństwa danych, jako główny dokument z zakresu SZBI, kompleksowo odnosi się jedynie do wąskiej kategorii bezpieczeństwa informacji, jakimi są dane osobowe, zaś w zakresie pozostałych danych nie cechuje jej podobny poziom złożoności i dokładności. Aktualność oraz kompleksowość dokumentacji SZBI jest podstawą prawidłowego funkcjonowania całego systemu oraz ochrony jednostki przed potencjalnymi naruszeniami.

Mając na uwadze powyższe, wskazany obszar należy ocenić **pozytywnie z nieprawidłowościami.**

2. Analiza zagrożeń związanych z przetwarzaniem informacji.

Regulacja zawarta w przepisie § 20 ust. 2 pkt. 3 r.k.r.i. wskazuje na konieczność przeprowadzania okresowych analiz ryzyka utraty integralności, dostępności lub poufności

informacji oraz podejmowania działań minimalizujących to ryzyko, stosownie do wyników przeprowadzonej analizy. Należy podkreślić, że analiza ryzyka jest istotnym elementem SZBI, umożliwia wskazanie zagrożeń związanych z przetwarzaniem informacji, a także ustalenie prawdopodobieństwa ich wystąpienia, czy stopień akceptacji ryzyka.

W pkt 2.2. ankiety dot. powyższego zagadnienia kierownik jednostki kontrolowanej wskazał, że:

> *„Tak - analiza jest prowadzona na potrzeby krytycznych systemów. Prowadzone są działania zapewniające poufność, integralność i dostępność (CIA) dla kluczowych elementów. Brakuje dokumentacji z tych działań. Ze względu na brak polityki nie istnieją udokumentowane wyniki."*

[dowód: akta kontroli str. 25]

Mając na uwadze powyższe należy podkreślić, iż kontrolowana jednostka nie udokumentowała, że przeprowadziła wymaganą § 20 ust. 2 pkt. 3 r.k.r.i. okresową analizę ryzyka utraty integralności, dostępności i poufności informacji oraz że zidentyfikowała ryzyka utraty poufności, rozliczalności oraz integralności danych przetwarzanych w systemach teleinformatycznych. Brak zatem dowodów potwierdzających, że w WUOZ zidentyfikowano w okresie objętym kontrolą ryzyka, ich poziom, sposób postępowania z nimi i podjęto działania minimalizujące ryzyko. Istotnym elementem prawidłowo przeprowadzonej analizy ryzyka jest również zapoznanie z jej treścią kierownika jednostki kontrolowanej.

Analiza ryzyka jest narzędziem służącym do zmniejszenia potencjalnego zagrożenia i jego wpływu na funkcjonowanie organizacji. Pozwala przede wszystkim na określenie poziomu zagrożenia, a dzięki temu podjęcie dobrze skrojonych działań zapobiegawczych lub eliminacyjnych. Podstawowe komponenty analizy to rozpoznanie ryzyka oraz zarządzanie nim.

Mając na uwadze powyższe niniejszy obszar należy ocenić ***negatywnie.***

3. Procedury zgłaszania incydentów naruszenia bezpieczeństwa informacji.

Przepis § 20 ust. 2 pkt 13 r.k.r.i. zobowiązuje podmiot realizujący zadania publiczne do zapewnienia warunków umożliwiających realizację i egzekwowanie bezzwłocznego zgłaszania incydentów naruszenia bezpieczeństwa informacji w określony i z góry ustalony sposób, umożliwiający szybkie podjęcie działań korygujących. Wymaga to ujęcia tej kwestii w regulacjach wewnętrznych jednostki, które powinny określać w sposób kompleksowy zasady zgłaszania oraz postępowania z incydentami, jak również prowadzenia rejestru incydentów, w celu ich identyfikacji.

W ankiecie dot. działania systemów teleinformatycznych w punkcie 2.3.1. wskazano, że:

> *„Nie istnieje określony sposób zgłaszania incydentów. Potencjalne incydenty są monitorowane przez oprogramowania AV Anty Malware oraz system monitoringu kluczowych elementów systemu Zabix."*

[dowód: akta kontroli str. 25-26]

Niemniej jednak, w toku czynności kontrolnych poproszono o przesłanie załącznika nr 21 (Instrukcję naruszeń[7]) do zarządzenia nr 6 z dnia 29 stycznia 2021 r.[8] (dalej jako zarządzenie z 2021 r.) Zgodnie z Instrukcją Naruszeń, w sytuacji naruszenia ochrony danych osobowych osobami odpowiedzialnymi za ochronę danych osobowych, zgodnie z właściwością są: Dolnośląski Wojewódzki Konserwator Zabytków, Zastępca Dolnośląskiego Wojewódzkiego Konserwatora Zabytków, IOD, ASI, KKO, osoby upoważnione do przetwarzania danych osobowych oraz osoby, które nie przetwarzają danych osobowych, ale w ramach czynności poznały sposoby ich zabezpieczenia. Instrukcja ta zawiera w głównej mierze zapisy dot. działania w przypadku naruszenia danych osobowych, zgodnie z którą każdy zobowiązany do ochrony danych osobowych, kto stwierdzi lub podejrzewa naruszenie zabezpieczenia danych osobnych powinien niezwłocznie poinformować o tym: właściwego KKO (brak definicji w Zarządzeniu i Instrukcji), którego obowiązkiem jest poinformowanie o naruszeniu Administratora lub osobę zastępującą, ASI i IOD lub bezpośrednio Administratora w sytuacjach szczególnych (...).

Instrukcja ta wprowadza oznaczenie m.in. Administratora i ASI. Funkcja Administratora nie jest przypisana wprost do konkretnej osoby/stanowiska. Dodatkowo, w § 2 ust. 7 Instrukcji w przypadku zdarzenia mającego związek z systemem informatycznym ASI zobowiązany jest do szczegółowej analizy systemu w celu potwierdzenia lub wykluczenia faktu naruszenia, wygenerowania, wydrukowania wszystkich możliwych dokumentów, raportów lub zestawień, które mogą pomóc w ustaleniu okoliczności zdarzenia, opatrując je datą i podpisem, fizycznego odłączenia urządzenia, segmentu sieci, które mogły umożliwiać dostęp do bazy danych osobowych osobie nieupoważnionej, wylogowania użytkownika podejrzewanego o naruszenie ochrony danych osobowych, zmiany haseł na konta, poprzez które uzyskano nielegalny dostęp oraz przywrócenie normalnego działania systemu (...). O podjętych działaniach powinien niezwłoczenie poinformować Administratora. W piśmie z dnia 6 czerwca 2023 r. znak WUOZ.1610.1.2023.DG wskazano zaś, że:

> *„W WUOZ nie został wyznaczony Administrator Systemów Informatycznych. Funkcji takiej nie wyznaczono, gdyż obowiązujące przepisy nie nakładają na organ takiego obowiązku; jest to jedynie uprawnienie administratora danych osobowych. W okresie kontroli WUOZ miał zawartą stałą umowę na usługi związane z utrzymaniem i administracją systemu IT."*

Mając na uwadze brak jednoznacznego wskazania, do której osoby należy zgłosić incydent (powyższe regulacje mogą wprowadzać w pracownika w błąd), należałoby w zapisach dotyczących zgłaszania incydentu wskazać jednoznacznie pracownika (lub jego zastępców) „pierwszego kontaktu", ze wskazaniem konkretnego stanowiska, który wstępnie przyjmuje takie zgłoszenie. Kontrolowany organ nie wskazał, czy prowadzi Rejestr Naruszeń Bezpieczeństwa. Niemniej jednak na etapie zastrzeżeń do projektu wystąpienia pokontrolnego kontrolowany organ oświadczył, że w okresie objętym kontrolą w WUOZ nie odnotowano naruszeń bezpieczeństwa informacji.

[dowód: akta kontroli str. 83-85]

---

[7] Instrukcja postępowania w sytuacji naruszenia ochrony danych osobowych – Załącznik nr 21 do Zarządzenia nr 6 z dnia 29 stycznia 2021 r. w sprawie wdrożenia procedur Ochrony Danych Osobowych (...).

[8] Zarządzenie nr 6 z dnia 29 stycznia 2021 r. w sprawie wdrożenia procedur Ochrony Danych Osobowych (...).

Podsumowując należy wskazać, iż w WUOZ określono procedury zgłaszania incydentów, jednak nie są one wystarczająco wyczerpujące i jednoznaczne. Mając na uwadze powyższe, wskazany obszar należy ocenić ***pozytywnie z nieprawidłowościami.***

4. Audyt wewnętrzny z zakresu bezpieczeństwa informacji.

Mając na uwadze § 20 ust. 2 pkt 14 r.k.r.i. podmiot realizujący zadania publiczne zobowiązany jest do zapewnienia okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji, nie rzadziej niż raz na rok. Audyt jest jednym z istotnych elementów wpływających na utrzymanie oraz doskonalenie całego SZBI. Pozwala na wskazanie mocnych i słabych stron przyjętych rozwiązań, a następnie ich analizę i podjęcie odpowiednich działań korygujących. Brak audytów uniemożliwia optymalne szacowanie istniejących ryzyk, jak również wyeliminowanie potencjalnych słabości, dlatego też tak ważne jest jego uregulowanie w dokumentach z zakresu bezpieczeństwa informacji.

Ponadto, audyt stanowi kluczowe narzędzie, które pozwala na regularny przegląd SZBI. Niezapewnienie przeprowadzania audytów wewnętrznych jest sprzeczne z § 20 ust. 1 r.k.r.i., który zobowiązuje podmiot realizujący zadania publiczne do monitorowania oraz przeglądania i doskonalenia SZBI. Aktualizacja regulacji wewnętrznych opiera się w znaczącym stopniu na przeprowadzanych audytach oraz realizacji zaleceń poaudytowych, a ich brak może skutkować pominięciem istotnych czynników wymagających zmiany.

Kontrola wykazała, iż w WUOZ nie przeprowadzano wymaganych corocznie audytów wewnętrznych (pkt 2.4 ankiety), wbrew zapisom § 20 ust. 2 pkt 14 r.k.r.i. Nie wykorzystano tym samym istotnego narzędzia, które pozwala na aktualizację i przegląd funkcjonującego SZBI, identyfikację potencjalnych zagrożeń, czy wykazania ewentualnych słabości istniejącego systemu. Zaznaczenia wymaga, iż kontroler w pytaniu z 31 maja 2023 r. prosił również o wskazanie przyczyn braku przeprowadzania audytu i powołania zespołu audytowego. W odpowiedzi z dnia 6 czerwca 2023 r. kontrolujący wskazał, że:

> *„W WUOZ nie są przeprowadzane audyty wewnętrzne systemów teleinformatycznych i nie został powołany zespół audytorów wewnętrznych w tym obszarze – WUOZ w systemach teleinformatycznych nie przetwarza informacji niejawnych. Pracownik posiadający uprawnienia do przetwarzania informacji niejawnych wykonuje swoje obowiązki w systemie analogowym (maszyna do pisania, pismo odręczne).”*

[dowód: akta kontroli str. 26, 100, 103]

Powyższe wyjaśnienia nie zasługują na uwzględnienie. Brak przeprowadzenia audytu wewnętrznego w zakresie bezpieczeństwa informacji nie rzadziej niż raz w roku stanowi naruszenie dyspozycji § 20 ust. 2 pkt 14 r.k.r.i. dot. potrzeby przeprowadzania regularnych audytów bezpieczeństwa informacyjnego.

Jak wskazano na wstępie, przedmiotowy audyt wewnętrzny ma na celu optymalne szacowanie istniejących ryzyk, jak również wyeliminowanie potencjalnych słabości występujących w obszarze bezpieczeństwa informacji. Kontrolowana jednostka nie posiada stosownych regulacji prawnych umożliwiających rozpoczęcie realizowania założeń wynikających z dyspozycji § 20 ust. 2 pkt 14 r.k.r.i..

Z powyższych względów niniejszy obszar oceniono ***negatywnie.***

5. Zarządzanie uprawnieniami do pracy w systemach informatycznych.

Istotnym elementem bezpieczeństwa informacji jest zarządzanie uprawnieniami. Proces ten ma zapewnić, że osoby zaangażowane w przetwarzanie informacji, posiadają stosowne uprawnienia i uczestniczą w tym procesie w stopniu adekwatnym do realizowanych zadań oraz obowiązków, a w przypadku zmiany/nierealizowania zadań następuje również zmiana/cofnięcie tych uprawnień.

Istotnym elementem bezpieczeństwa informacji jest zarządzanie uprawnieniami. Proces ten ma zapewnić, że osoby zaangażowane w przetwarzanie informacji, posiadają stosowne uprawnienia i uczestniczą w tym procesie w stopniu adekwatnym do realizowanych zadań oraz obowiązków, a w przypadku zmiany/nierealizowania zadań następuje również zmiana/cofnięcie tych uprawnień.

W toku kontroli sprawdzono, czy osoby zaangażowane w proces przetwarzania informacji w WOUZ we Wrocławiu posiadają stosowne uprawnienia i uczestniczą w tym procesie w stopniu adekwatnym do realizowanych przez nie zadań oraz obowiązków mających na celu zapewnienie bezpieczeństwa informacji, zgodnie z § 20 ust. 2 pkt 4 rozporządzenia KRI.

W WUOZ we Wrocławiu do obsługi kadr i płac jest używany program Progman. Do programu Progman w zakresie kadr i płac dostęp mają jedynie Panie J.Ż, J.W oraz B.W. będące aktualnie pracownikami WOUZ.

W ankiecie dotyczącej działania systemów teleinformatycznych używanych do realizacji zadań podmiotu, kontrolowany organ zaznaczył:

> *„Brak regulacji wewnętrznych dotyczących uprawnień użytkowników. Dobre praktyki z zakresu ograniczania uprawnień są wdrożone na krytycznych systemach poprzez ograniczenie uprawnień kont użytkowników."*

W kontrolowanej jednostce nie funkcjonuje wniosek ani pisemne upoważnienie o nadanie/zmianę/odebranie uprawnień dostępu do systemów teleinformatycznych WUOZ we Wrocławiu.

Czynności kontrolne wykazały, że osoby J.Ż. i J.W. posiadały uprawnienia do systemu Progman w pełnym zakresie.

[dowód: akta kontroli str. 126-127]

Ponadto w wyniku kontroli ustalono, iż na kontrolowanych komputerach użytkownicy pracują na kontach imiennych i nie posiadają uprawnień administracyjnych, co należy ocenić pozytywnie.

[dowód: akta kontroli str. 121-123]

Mając na uwadze powyższe ustalenia obszar zarządzania uprawnieniami do pracy w systemach teleinformatycznych oceniono ***pozytywnie.***

6. Praca na odległość i mobilne przetwarzanie danych.

W ankiecie dotyczącej działania systemów teleinformatycznych używanych do realizacji zadań podmiotu kontrolowany organ zaznaczył:

> *„Przetwarzanie mobilne odbywa się tylko na wydzielonych urządzeniach mobilnych – laptopy. Komunikacja zdalna jest chroniona przez szyfrowane połączenia VPN. Brak dokumentacji w tym zakresie."*

[dowód: akta kontroli str. 26]

W toku czynności kontrolnych poproszono kierownika jednostki kontrolowanej o przedłożenie załącznika nr 26 do Zarządzenia nr 6 z dnia 29 stycznia 2021 r., stanowiącego Regulamin pracy zdalnej. Regulamin zawiera wszystkie zagadnienia niezbędne do zapewnienia bezpiecznej pracy zdalnej, jednakże niektóre obszary wymagają doprecyzowania lub uzupełnienia. Należy zwrócić szczególną uwagę na komputery prywatne, wykorzystywane do pracy zdalnej, ponieważ mogą one nie mieć ustawionych takich zabezpieczeń jak komputery służbowe np. mogą nie mieć wygaszacza ekranu, wymuszonej zmiany hasła itd. Wymóg wskazujący, że hasło musi zawierać 6 znaków jest niewystarczający do utworzenia silnego, bezpiecznego hasła, wobec czego należałoby dodać wymaganie dotyczące złożoności haseł np. co najmniej 1 cyfra, znak specjalny, duża i mała litera. Rekomendowane jest zwiększenie długości hasła do co najmniej 8 znaków oraz wprowadzenie obowiązku regularnej zmiany hasła np. raz w miesiącu. Wymóg dotyczący przesyłania plików w postaci załączników zabezpieczonych hasłem nie gwarantuje zachowania poufności przesyłanych informacji. Należy dodać wymaganie, aby dane były przed wysłaniem zaszyfrowane oraz żeby hasło do odszyfrowania było przekazywane innym kanałem komunikacji np. telefonicznie. Stwierdzono również nw. braki: wymogu, aby system operacyjny Windows komputera, używanego do pracy zdalnej był wspierany przez producenta oraz był na bieżąco aktualizowany; wymogu, aby komputer używany do pracy zdalnej był regularnie skanowany pod kątem obecności wirusów, np. raz w tygodniu; wymogu, aby komputer używany do pracy zdalnej miał włączony wygaszacz ekranu, uruchamiany automatycznie po określonym czasie w przypadku braku aktywności użytkownika, a monitor zestawu komputerowego był ustawiony w sposób uniemożliwiający osobom postronnym wgląd w dane wyświetlane na ekranie. Ponadto, rekomendowane jest wprowadzenie wyraźnego zakazu podłączania prywatnych nośników do komputera służbowego, używanego do pracy zdalnej oraz wprowadzenie wyraźnego zakazu zapisywania danych służbowych na prywatnym komputerze, używanym do pracy zdalnej.

[dowód: akta kontroli str. 86-89]

W zestawieniu systemów teleinformatycznych używanych do realizacji zadań zleconych kontrolowany organ zaznaczył, że pracę na odległość i mobilne przetwarzanie danych w systemie eDOK zapewnia szyfrowane połączenie VPN z delegatur i dla upoważnionych pracowników realizowane przez router softwareowy, wykazany w pozycji nr 11 Zestawienia.

[dowód: akta kontroli str. 121-123]

W kontrolowanej jednostce nie funkcjonuje wniosek, ani pisemne upoważnienie o nadanie/zmianę/odebranie uprawnień do pracy zdalnej, istnieje jednakże rejestr poboru nośników danych, będący załącznikiem nr 26 A do Zarządzenia z dnia 29 stycznia 2021 r.

[dowód: akta kontroli str. 88]

Kontrola wykazała, iż jednostka kontrolowana przedstawiła ustanowione podstawowe zasady zapewniające bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość, zgodnie z § 20 ust. 2 pkt 8 r.k.r.i.

Odnosząc się do ustalonego powyżej stanu faktycznego należy pozytywnie ocenić fakt wykonywania pracy zdalnej przez szyfrowane kanały VPN istotne dla kwestii dotyczących bezpieczeństwa informacji.

Mając na uwadze powyższe, zagadnienie pracy na odległość i mobilnego przetwarzania danych oceniono **pozytywnie z nieprawidłowościami.**

7. Zabezpieczenia techniczno-organizacyjne dostępu do informacji.

Kontrola wykazała, że budynek, w którym mieści się siedziba WUOZ stanowi własność Skarbu Państwa w wieczystym użytkowaniu. Przeprowadzone czynności kontrolne wykazały, iż dostęp do budynku nie jest w żaden sposób ograniczony, ale tylko w zakresie dostępu do biura podawczego mieszczącego się na parterze budynku nr 11 przy ul. Władysława Łokietka we Wrocławiu. Aby dostać się do pozostałych pomieszczeń należy posiadać kartę dostępu lub być wprowadzonym przez pracownika. Siedziba WUOZ ma zapewnioną fizyczną ochronę, niemniej jednak jest ona dostępna na wezwanie. Należy zatem stwierdzić, iż w kontrolowanej jednostce ruch osobowy jest monitorowany oraz podjęto środki w celu minimalizacji ryzyka wystąpienia kradzieży informacji.

Ponadto, w wyniku kontroli stwierdzono, iż w Zarządzeniu nr 39/ 2019 z 3 grudnia 2019 r. określono następujące rodzaje zabezpieczeń techniczno-organizacyjnych, zawarte w Polityce Bezpieczeństwa Informacji i Systemów Teleinformatycznych w WUOZ we Wrocławiu (dalej jako PBI):

- nakaz zabezpieczenia dostępu każdego systemu informatycznego dopuszczonego do pracy w WUOZ tylko dla osób upoważnionych (§ 4 ust. 1 pkt 1 PBI),
- nakaz aby każdy element systemu informatycznego był podpięty do gniazd wydzielonej sieci elektrycznej, a jednostki szczególnie ważne także do awaryjnych zasilaczy UPS, co ma chronić przetwarzane na nich dane przed utratą integralności, a jednostkę przed utratą ciągłości działania (§ 4 ust. 1 pkt 2 PBI),
- zastrzeżenie prawa do wykonywania napraw i modyfikacji tylko do osób upoważnionych
(§ 4 ust. 1 pkt 3 PBI),
- zmiany w strukturze, położeniu i ustawieniach urządzeń są wykonywane wyłącznie za wiedzą i zgodą administratora (§ 4 ust. 1 pkt 4 PBI),
- okablowanie strukturalne sieci służy wyłącznie obsłudze urządzeń teleinformatycznych WUOZ, a miejsca jego połączenia powinny być szczególnie chronione, natomiast nieużywane gniazda powinny być nieaktywne lub w uzasadnionych przypadkach przyporządkowane do określonego obszaru z odseparowaniem od sieci głównej (§ 4 ust. 1 pkt 5, pkt 7 i pkt 8 PBI),
- bez zgody i wiedzy administratora nie można podłączać ani odłączać jakichkolwiek urządzeń (§ 4 ust. 1 pkt 6 PBI),
- osoby nieupoważnione nie mogą pozostawać bez nadzoru w pomieszczeniach, w których znajdują się urządzenia systemu teleinformatycznego (§ 4 ust. 1 pkt 9 PBI),
- styk sieci wewnętrznej WUOZ z siecią publiczną jest chroniony przez zaporę (§ 4 ust. 1 pkt 10 PBI),
- korzystanie z sieci publicznej może się odbywać wyłącznie w celach służbowych (§ 4 ust. 1 pkt 11 PBI).

Poza powyższym, w Zarządzeniu z 2019 r. określono zakres zabezpieczeń obejmujących serwerownię i znajdująca się tam infrastrukturę, na które składają się:

- lokalizacja serwerowni w odrębnym i zamykanym pomieszczeniu, do której dostęp wymaga odnotowania w rejestrze wydawanych kluczy oraz odbywa się wyłącznie w obecności administratora lub upoważnionej osoby (§ 4 ust. 2 pkt 1 - pkt 3 PBI),
- serwery WUOZ, wraz z osprzętem, są umieszczone w zamykanych szafach, do których klucze są umieszczone w sejfie podręcznym poza serwerownią, a dostęp do nich mają wyłącznie osoby wskazane przez kierownika kontrolowanej jednostki (§ 4 ust. 2 pkt 4 i pkt 5 PBI),
- ciągłość działania serwerowni zapewniają zasilacze UPS a hasła administracyjne są w bezpieczny sposób przechowywane przez kierownika kontrolowanej jednostki (§ 4 ust. 2 pkt 6 i pkt 8 PBI).

W zakresie poszczególnych stacji roboczych w Zarządzeniu z 2019 r. nakazano, aby każda z nich była chroniona wygaszaczem ekranu oraz hasłem dostępu, a tam gdzie jest to technicznie możliwe hasło dostępu wprowadza się także na poziomie poszczególny aplikacji (§ 4 ust. 3 pkt 2 i pkt 3 PBI). Ponadto, stacje robocze powinny być wyposażone w oprogramowanie antywirusowe zapewniające skanowanie dysków, nośników zewnętrznych oraz poczty email (§ 4 ust. 3 pkt 4 PBI). W WUOZ funkcjonuje polityka haseł określająca minimalne wymogi dla hasła w tym zasady jego tworzenia, częstotliwość jego zmian oraz zasady jego przechowywania.

W pkt 2.7.1. ankiety, kierownik kontrolowanej jednostki wskazał, iż dostęp do informacji przetwarzanych w kluczowych systemach nie jest wystarczająco monitorowany, brak jest możliwości wykrycia nieautoryzowanych działań (brak rozliczalności), informacje nie są częściowo zabezpieczone przez nieuprawnioną modyfikacją (brak integralności) oraz nie są zabezpieczone przez nieuprawnionym ujawnieniem (brak poufności), informacje nie są zabezpieczone przez nieuprawnionym zniszczeniem (brak dostępności), wobec czego na niektórych systemach wymagane jest podniesienie jakości zabezpieczeń.
[dowód: akta kontroli str. 27, 72-77]

Odnosząc się do ustalonego powyżej stanu faktycznego należy pozytywnie ocenić środki zabezpieczenia technicznego dostępu do pomieszczeń WUOZ, w tym szczególnie do serwerowni, co wskazuje, że w tym zakresie podjęto odpowiednie działania zapewniające ochronę przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami poprzez monitorowanie dostępu do informacji, zgodnie z przepisem § 20 ust. 2 pkt 7 lit. a r.k.r.i. Powyższe rozwiązania zasługują również na pozytywną ocenę, albowiem stanowią wypełnienie dyspozycji przepisu § 20 ust. 2 pkt 11 r.k.r.i. Niemniej jednak, z uwagi na nieprawidłowości, na jakie sam wskazał w ankiecie kierownik kontrolowanej jednostki, niniejszy obszar należy ocenić ***pozytywnie z nieprawidłowościami.***

8. Zabezpieczenia techniczno-organizacyjne systemów informatycznych.

Zgodnie z przepisem § 20 ust. 2 pkt 7 lit. b i c r.k.r.i. zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienie przez kierownictwo podmiotu publicznego warunków umożliwiających realizację i egzekwowanie zapewnienia ochrony przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami, przez czynności zmierzające do wykrycia nieautoryzowanych działań

związanych z przetwarzaniem informacji, a także zapewnienie środków uniemożliwiających nieautoryzowany dostęp na poziomie systemów operacyjnych, usług sieciowych i aplikacji.

Kontrolowana jednostka nie przedstawiła wewnętrznych uregulowań w powyższym zakresie. W Ankiecie dotyczącej działania systemów teleinformatycznych używanych do realizacji zadań podmiotu, kontrolowany organ zaznaczył: Brak zdefiniowanych polityk. Kontrola systemu tylko względem dobrych praktyk.

W toku kontroli w WOUZ we Wrocławiu ustalono, iż na kontrolowanych komputerach B.W., J.W. i J.Ż. był zainstalowany program antywirusowy ESET32. Wobec stale rosnącego poziomu zagrożeń należy rozważyć wdrożenie bardziej zaawansowanej ochrony antywirusowej np. ESET Endpoint Security oraz centralnego systemu zarządzania. Używanie programu Endpoint Security zwiększa poziom bezpieczeństwa stacji roboczych przez zastosowanie dodatkowych mechanizmów zabezpieczeń w postaci dwukierunkowego firewall, kontrolę dostępu do stron WWW oraz ochronę przed botnetami. Centralne zarządzanie systemem antywirusowym przyspiesza proces powiadomienia o zdarzeniach na komputerach użytkowników. Kontrola wykazała używanie wygaszacza ekranu i aktualizację ochrony antywirusowej. Na kontrolowanych komputerach wygaszacz ekranu jest ustawiony na 10 minut.

[dowód: akta kontroli str. 138-143]

Kontrola programów e-dok i Progman na komputerze pracownika (K.D.) wykazała, iż posiadły one wdrożoną politykę haseł. Program e-dok wymaga hasła 8-znakowego z dużymi literami i cyframi o ważności 30 dni i niepowtarzalności z ostatnim. Z kolei program Progman wymusza minimalną liczbę znaków 8, użycie przynajmniej jednej wielkiej litery, cyfry i innego znaku, ważność przez 30 dni i niepowtarzalność hasła w ciągu 6 zmian. Oba systemy posiadają złożone mechanizmy ustawień polityki haseł, które umożliwiają zwiększenie poziomu bezpieczeństwa np. ustawienie blokady obecności loginu w hasłach.

[dowód: akta kontroli str. 124-125]

Kontrolowane programy pracują w środowisku wirtualnym Hyper_v. Środowisko wirtualne składa się z fizycznych serwerów, które zapewniają redundancje względem siebie. Zastosowanie klastrowego środowiska wirtualnego zwiększa poziom dostępności i bezpieczeństwa systemów.

Ocenie poddano również stosowane mechanizmy ochrony przed błędami, utratą, nieuprawnioną modyfikacją. Ustalono, iż sieć w WOUZ we Wrocławiu jest zabezpieczona na styku z Internetem poprzez sprzętowy firewall. Wobec stale rosnącego poziomu zagrożeń należy rozważyć zastosowanie na styku z Internetem dedykowanego urządzenia, które dostarcza wielu funkcjonalności takich: firewall, IPS (ochrona przed atakami), filtrowanie treści WWW, antywirus, VPN, kontrola aplikacji, optymalizacja pasma czy ochrona przed spamem.

Oględzinom poddano serwerownię WOUZ we Wrocławiu, która znajduje się na drugim piętrze budynku. Wejście do serwerowni poprzedza pomieszczenie biurowe, zamykane na klucz. Serwerownia nie jest zabezpieczona system kontroli dostępu, nie ma systemu detekcji dymu, nie jest objęta systemem monitoringu wizyjnego. Serwerownia posiada system alarmowy, klimatyzację bez redundancji oraz system zasilania awaryjnego UPS, który podtrzymuje pracę urządzeń przez około 20 minut. W serwerowni znajduje się jedna szafa teleinformatyczna, która

nie jest zabezpieczona system kontroli dostępu. Stwierdzony stan faktyczny udokumentowano w protokole oględzin, a także w materiale poglądowym.
[dowód: akta kontroli str. 91-92]

Odnosząc się do ustalonego powyżej stanu faktycznego stwierdzono, że kontrolowany organ zasadniczo zapewnia ochronę przetwarzanych informacji zgodnie z przepisem § 20 ust. 2 pkt 7 lit. a r.k.r.i., mając jednak na względzie stwierdzone nieprawidłowości zagadnienie oceniono **pozytywnie z nieprawidłowościami.**

9. Rozliczalność działań w systemach teleinformatycznych.

Rozliczalność jest właściwością systemu pozwalającą przypisać określone działanie w systemie do osoby fizycznej lub procesu oraz umiejscowić je w czasie. Z tego względu zapewnienie rozliczalności działań polega na gromadzeniu informacji o tym, kto, kiedy i jakie czynności wykonał w systemie. Obligatoryjnie podlegają dokumentowaniu w postaci zapisów w dziennikach systemów (logi) wszystkie działania dostępu do systemu z uprawnieniami administracyjnymi, w zakresie konfiguracji systemu i zabezpieczeń, a także działania, gdy przetwarzanie danych podlega prawnej ochronie.

Zgodnie z § 21 ust. 2 r.k.r.i. w dziennikach systemowych należy odnotowywać działania użytkowników lub obiektów systemowych polegające na dostępie do systemu z uprawnieniami administracyjnymi, konfiguracji systemu, w tym konfiguracji zabezpieczeń, przetwarzanych w systemach danych podlegających prawnej ochronie w zakresie wymaganym przepisami prawa.

Kontrolowana jednostka nie przedstawiła wewnętrznych uregulowań w powyższym zakresie. W ankiecie dotyczącej działania systemów teleinformatycznych używanych do realizacji zadań podmiotu kontrolowany organ zaznaczył: Brak informacji o rodzaju danych przetwarzanych w systemach; Brak ustalonej polityki przechowywania logów.

W wyniku kontroli stwierdzono że w kontrolowanych systemach – eDOK oraz Progman rozliczalność jest zapewniona.

W systemie eDOK rozliczalność w zakresie dostępu do dokumentów, edycji, powiązań dokumentów i ich przekazywania, dostępne są w opcji Metryka widocznej przy menu każdej paczki dokumentów (sprawy) zawierającej: datę i czas wykonanej czynności, imienne oznaczenie osoby wykonującej czynność oraz rodzaj wykonanej czynności.

W systemie Progman rozliczalność jest dostępna w postaci Rejestru operacji, zawierającego: imienne oznaczenie osoby wykonującej czynność, datę i czas wykonanej czynności oraz jej rodzaj. Rejestr operacji jest sparametryzowany, więc można wybrać przedział czasowy, osobę wykonującą czynność oraz moduł systemu Progman, w którym czynność była wykonywana.
[dowód: akta kontroli str. 128-129]

Mając na uwadze powyższe ustalenia zagadnienie zostało ocenione **pozytywnie z nieprawidłowościami.**

10. Kopie zapasowe.

Zgodnie z § 20 ust. 2 pkt 12 lit. b) i e) r.k.r.i. zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienie przez kierownictwo podmiotu publicznego

warunków umożliwiających realizację i egzekwowanie m.in. zapewnienia odpowiedniego poziomu bezpieczeństwa w systemach teleinformatycznych, polegającego w szczególności na minimalizowaniu ryzyka utraty informacji w wyniku awarii i zapewnieniu bezpieczeństwa plików systemowych. Do realizacji tego obowiązku niezbędne jest opracowanie odpowiednich procedur i podjęcie określonych w nich działań polegających na zabezpieczaniu przetwarzanych przez jednostkę danych poprzez tworzenie kopii zapasowych zbiorów danych.

Ustalono, iż w WUOZ we Wrocławiu określono wewnętrznie obowiązek sporządzania kopii zapasowych w § 4 Polityki Bezpieczeństwa Informacji i Systemów Teleinformatycznych w WUOZ we Wrocławiu, w części odnoszącej się do bezpieczeństwa danych i systemów informatycznych. Zgodnie z § 4 ust. 2 pkt 9 PBI „dla zapewnienia ciągłości działania urzędu wykonuje się kopie zapasowe strategicznych danych, wykonywaną przez Administratora Systemów Komputerowych za pomocą dedykowanego systemu kopii zapasowych (Bacula) oraz w formie replik blokowych dla kluczowych systemów, repliki są wykonywane na lokalizacji zdalnej". W § 4 ust. 3 pkt 5 PBI postanowiono, iż "bezpieczeństwo danych przetwarzanych w urzędzie zapewnione jest poprzez wykonywanie kopii zapasowych danych za pomocą dedykowanego systemu kopii zapasowych (Bacula) oraz w formie replik blokowych dla kluczowych systemów, repliki są wykonywane na lokalizacji zdalnej".
[dowód: akta kontroli str. 75]

Stwierdzono, iż zapisy PBI nie uwzględniają częstotliwości wykonywania kopii zapasowych, ani miejsca ich przechowywania. Przyjęte zasady powinny uwzględniać szczegółowo działania związane z wykonywaniem, przechowywaniem i testowaniem kopii zapasowych danych i systemów, aby wypełnić normę § 20 ust. 3 r.k.r.i.. Braki w opisanych powyżej zakresie skutkują tym, iż kopie zapasowe mogą być wykonywane oraz usuwane w sposób niezorganizowany i niesformalizowany, uniemożliwiający jakąkolwiek weryfikację i rozliczalność zasadności i poprawności przeprowadzenia powyższych działań. Podobnie w kwestii okresu przechowywania kopii zapasowych oraz weryfikacji ich przydatności do dalszego użytku.

W przekazanej w załączeniu do pisma z dnia 19 maja 2023 r. ankiecie dotyczącej działania systemów teleinformatycznych używanych do realizacji zadań podmiotu, kontrolowany organ wskazał, iż „system posiada kopie zapasowe, repliki czasu rzeczywistego, w tym repliki czasu rzeczywistego z rozproszeniem geograficznym dla kluczowych systemów".
[dowód: akta kontroli str. 30]

W wyniku kontroli ustalono, iż tworzenie kopii zapasowych wykonywane jest regularnie.

W toku czynności kontrolnych ustalono, iż kopie zapasowe są przechowywane w serwerowni WUOZ we Wrocławiu i posiadają dwie repliki, w tym jedną w delegaturze w Wałbrzychu. W wyniku dokonanych oględzin ustalono, iż kopie zapasowe systemów teleinformatycznych są przetrzymywane na przestrzeni dyskowej w serwerowni WUOZ we Wrocławiu i są dodatkowo kopiowane na taśmy magnetyczne. Kopie są wykonywane za pomocą programu Bacula. Kopie na dyskach są przechowywane przez 3 miesiące, a na taśmach przez pół roku. Dane przyrostowe systemów są wykonywane codziennie, a dane użytkowników 1 lub 2 razy dziennie. Pełne kopie są wykonywane raz w tygodniu.
[dowód: akta kontroli str. 90]

Kontrola wykazała, że kopie przyrostowe bazy danych systemu eDOK są wykonywane o godzinie 12, 15 i 18, a kopie przyrostowe programu Progman o godzinie 18. Kopie

przyrostowe użytkownika E.M. są wykonywane codziennie o 13:30, a użytkownika K.M. codziennie o 14:00.
[dowód: akta kontroli str. 144-153]

Wobec powyższych ustaleń stwierdzono, iż jednostka kontrolowana minimalizuje ryzyko utraty informacji w wyniku awarii tworząc kopie zapasowe oraz zapewnia bezpieczeństwo plików systemowych, czym zapewnia odpowiedni poziom bezpieczeństwa w systemach teleinformatycznych, zgodnie z § 20 ust. 2 pkt 12 lit. b) i e) r.k.r.i. Negatywnie należy ocenić brak regulacji wewnętrznych dot. formalnych zasad tworzenia, przechowywania oraz testowania utworzonych kopii zapasowych danych i systemów podmiotu. Nie wskazano również zakresu wykonywania kopii zapasowych na stacjach roboczych. Nie określono kto i w jakim zakresie jest odpowiedzialny za sporządzanie i bezpieczeństwo kopii zapasowych. Przyjęte zasady powinny uwzględniać szczegółowo działania związane z wykonywaniem, przechowywaniem i testowaniem kopii zapasowych danych i systemów, aby wypełnić normę § 20 ust. 3 rozporządzenia KRI.

Mając na uwadze powyższe ustalenia zagadnienie zostało ocenione **pozytywnie z nieprawidłowościami.**

11. Inwentaryzacja sprzętu i oprogramowania informatycznego.

Zgodnie z § 20 ust. 2 pkt 2 r.k.r.i. zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez utrzymywanie aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji obejmującej ich rodzaj i konfigurację. Posiadanie takich informacji jest niezbędne przy wprowadzaniu wszelkich zmian w środowisku informatycznym. Jednocześnie należy podkreślić, że ww. baza nie jest tożsama z zapisami księgi inwentarzowej. Zawiera ona bowiem, w szczególności informacje o wszystkich zidentyfikowanych aktywach informatycznych, w tym: szczegółowe dane o urządzeniach technicznych, oprogramowaniu i środkach komunikacji, ich rodzaju, parametrach, aktualnej konfiguracji i relacjach między elementami konfiguracji oraz użytkowniku.

W przekazanej w załączeniu do pisma z dnia 19 maja 2023 r. ankiecie dotyczącej działania systemów teleinformatycznych używanych do realizacji zadań podmiotu, organ kontrolowany wskazał, iż: *„brak takiej inwentaryzacji".*
[dowód: akta kontroli str. 30]

W wyniku kontroli ustalono, iż w okresie objętym kontrolą w WUOZ nie wykonywano inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji. W toku kontroli nie przedłożono żadnych dokumentów potwierdzających, że w WUOZ utrzymywana jest aktualność inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji obejmującej ich rodzaj i konfigurację. Kontrolowany organ wskazał, iż:

> *„Inwentaryzacja nie była wykonywana w przedmiotowej formie. Na koniec roku 2022 wcześniej wspomniane wypowiedzenie porozumienie w sprawie Miejskiego Konserwatora Zabytków wymusiło wykonanie innych priorytetów. Inwentaryzacja we właściwej formie zostanie przeprowadzona do końca 2023 r.".*

[dowód: akta kontroli str. 136]

W związku z powyższym wyjaśnić należy, że problemy organizacyjne jednostki nie mogą stanowić uzasadnienia zaniechania realizacji obowiązków, lecz należy je traktować jako powód powstania przedmiotowych nieprawidłowości.

Wobec dokonanych ustaleń należy uznać, iż kontrolowany podmiot nie podejmował działań w celu wypełnienia dyspozycji przepisu § 20 ust. 2 pkt 2 rozporządzenia r.k.r.i. W świetle powyższego zagadnienie należy ocenić **negatywnie.**

12. Serwis sprzętu informatycznego i oprogramowania.

Przepis § 20 ust. 2 pkt 10 r.k.r.i. przewiduje, że umowy serwisowe podpisane ze stronami trzecimi powinny zawierać zapisy gwarantujące odpowiedni poziom bezpieczeństwa informacji. W odniesieniu do systemów teleinformatycznych i oprogramowania o znaczeniu krytycznym dla funkcjonowania jednostki niezbędne jest objęcie ich (w zakresie zarówno oprogramowania użytkowego i systemowego, jak i sprzętu) stosownymi umowami serwisowymi, aby zapewnić gwarancję odpowiednio szybkiego wznowienia pracy systemów w przypadku wystąpienia awarii. Umowy takie, zgodnie z § 20 ust. 2 pkt 10 r.k.r.i. powinny posiadać zapisy gwarantujące odpowiedni poziom bezpieczeństwa informacji, w przypadku wejścia w ich posiadanie przez podmioty serwisujące.

W przekazanej w załączeniu do pisma z dnia 19 maja 2023 r. ankiecie dotyczącej działania systemów teleinformatycznych używanych do realizacji zadań podmiotu kontrolowany organ wskazał na *„brak stosownych zapisów”*.

[dowód: akta kontroli str. 29]

W wyniku kontroli ustalono, iż w okresie objętym kontrolą nie zawarto umów serwisowych, ani umów powierzenia danych osobowych z usługodawcami systemów zewnętrznych. Kontrolowany organ wyjaśnił, iż:

> *„WUOZ nie wykorzystuje żadnych systemów zewnętrznych (z zewnętrznym składowaniem danych). W związku z powyższym nie są wymagane umowy powierzenia danych - w załączeniu ogólne warunki umowy dotyczące korzystania z oprogramowania linii Progman (załącznik nr 7). Dane wymieniane pomiędzy siedzibą główną (Wrocław) a Delegaturami są transmitowane w szyfrowanych kanałach VPN.”*

[dowód: akta kontroli str. 104]

W ramach obsługi/serwisu stacji roboczych przekazano umowę zawartą pomiędzy Dolnośląskim Wojewódzkim Konserwatorem Zabytków (zleceniodawcą) a Quadricom Systemy Informatyczne NIP 8992389659 (zleceniobiorcą): umowę z dnia 8 stycznia 2018 r. (zmienianą aneksami) na usługi obsługę stacji roboczych oraz administrowania BIP urzędu. Analizując problem zagwarantowania w umowie odpowiedniego poziomu bezpieczeństwa informacji stwierdzono, że umowa (ani zawarte aneksy) nie zawierają klauzul dotyczących zachowania poufności informacji uzyskanych w trakcie realizacji umowy przez podmiot zewnętrzny. Wskazać wymaga, iż w przypadku zawieranych umów cywilnoprawnych z usługobiorcami istotne jest zawarcie w ich treści postanowień zabezpieczających w zakresie właściwego poziomu ochrony i bezpieczeństwa informacji przez nich uzyskanych. Ponadto zauważyć należy, iż § 6 PBI we Wrocławiu przewiduje obowiązkowe zapisy, które wprowadza się w umowach zawieranych z podmiotami zewnętrznymi. Przekazana natomiast umowa powierzenia danych osobowych z ww. podmiotem zewnętrznym (umowa z dnia 1 czerwca

2018 r.) po pierwsze nie wypełnia w sposób wystarczający art. 28 ust. 3 RODO (nie określa np. rodzaju przetwarzanych danych osobowych), a po drugie dotyczy innej umowy głównej – z dnia 1 lipca 2013 r. o utrzymanie i administrację systemu IT.

[dowód: akta kontroli str. 111-120]

Mając na uwadze, iż zawarta przez kontrolowany organ umowa z usługodawcą Quadricom Systemy Informatyczne nie zawiera zapisów gwarantujących odpowiedni poziom bezpieczeństwa informacji, zagadnienie oceniono **negatywnie.**

13. Szkolenia pracowników zaangażowanych w proces przetwarzania informacji.

Przepis § 20 ust. 2 pkt 6 r.k.r.i. nakłada wymóg zapewnienia szkolenia osób zaangażowanych w proces przetwarzania informacji, ze szczególnym uwzględnieniem takich zagadnień jak: zagrożenia bezpieczeństwa informacji (lit. a), skutki naruszenia zasad bezpieczeństwa informacji, w tym odpowiedzialność prawna (lit. b), stosowanie środków zapewniających bezpieczeństwo informacji, w tym urządzenia i oprogramowanie minimalizujące ryzyko błędów ludzkich (lit. c).

W wyniku kontroli ustalono, że organ kontrolowany nie organizował w okresie objętym kontrolą cyklicznych szkoleń z obszaru bezpieczeństwa informacji osób zaangażowanych w proces przetwarzania informacji, stosownie do § 20 ust. 2 pkt 6 r.k.r.i. W przekazanej w załączeniu do pisma z dnia 19 maja 2023 r. ankiecie dotyczącej działania systemów teleinformatycznych używanych do realizacji zadań podmiotu, organ kontrolowany wskazał: *„brak stosownych szkoleń dla pracowników".*

[dowód: akta kontroli str. 30]

W toku kontroli ustalono, iż określono zasady dotyczące zapewnienia wiedzy pracownikom z obszaru ochrony danych osobowych w dokumencie o nazwie „zasady organizacji edukacji z zakresu ochrony danych osobowych w WUOZ we Wrocławiu". Wprowadzono cztery rodzaje działań edukacyjnych: szkolenie przed przystąpieniem do pracy/stażu/praktyk, instruktaż stanowiskowy w zakresie ochrony danych osobowych, informowanie o zmianach w zakresie ochrony danych osobowych oraz szkolenie fakultatywne. Kontrolowany organ wskazał, iż:

> *„W jednostce kontrolowanej jest stosowana polityka i regulacja szkoleń w procesie przetwarzania informacji w systemach teleinformatycznych, która jest wdrożona w politykę szkoleń i stosowania Polityki Ochrony Danych Osobowych w WUOZ we Wrocławiu w związku ze stosowaniem przepisów RODO. W toku szkolenia pracownicy są szkoleni i informowani m.in. z zakresu ochrony danych osobowych, ich przetwarzania w systemie informatycznym i nie informatycznym, konieczności zabezpieczenia danych oraz procedur awaryjnych na wypadek ich utraty etc."*

[dowód: akta kontroli str. 136]

W toku kontroli ustalono, iż zapewniono szkolenia osobom nowozatrudnionym w zakresie ochrony danych osobowych. Kontrolowany wskazał, iż:

> *„Każdy nowo zatrudniony pracownik WUOZ przechodzi pełne szkolenie RODO, w ramach którego uwzględnia się kwestie zagrożenia bezpieczeństwa informacji, skutki naruszenia bezpieczeństwa informacji, w tym odpowiedzialność prawna stosowanie środków zapewniających*

bezpieczeństwo informacji, w tym urządzenia i oprogramowanie minimalizujące ryzyko błędów ludzkich (usuwalne klucze kryptograficzne do podpisu certyfikowanego, system antywirusowy). Szkolenie odbywaną się indywidualnie, jako szkolenia stanowiskowe. Nie prowadzimy rejestru/zestawienia szkoleń stanowiskowych".

[dowód: akta kontroli str. 104]

Przekazane w toku kontroli dokumenty o nazwie *„Potwierdzenie udziału w szkoleniu"* dla przeszkolonych pracowników potwierdzają realizację szkoleń wstępnych. Z treści przekazanych dokumentów wynika, iż w trakcie szkolenia zapoznano pracowników z regulacjami prawnymi w zakresie ochrony danych osobowych oraz regulacjami wewnętrznymi z zakresu ochrony danych osobowych obowiązujących w WUOZ. Pracownicy złożyli również stosowne oświadczenia o zobowiązaniu się do przestrzegania zasad dotyczących ochrony i bezpieczeństwa danych osobowych, co jest istotnym elementem dla ewentualnego skutecznego egzekwowania przez pracodawcę odpowiedzialności za naruszenie obowiązków wynikających z wewnętrznych regulacji.

[dowód: akta kontroli str. 93-99]

Należy natomiast podkreślić, iż pojęcie ochrony danych osobowych jest pojęciem węższym od pojęcia bezpieczeństwa informacji. Zauważyć należy, iż kontrolowany organ w § 5 ust. 1 PBI, wyodrębnił pięć grup przetwarzanych informacji w WUOZ (informacje niejawne, dane osobowe, informacje pozyskane w związku z zawartymi umowami, porozumieniami itp., informacje wewnętrzne, informacje publiczne). Ochrona danych osobowych jest jednym z elementów wchodzących w skład bezpieczeństwa informacji.

Wskazać wymaga, iż stałe podnoszenie świadomości pracowników w zakresie zagrożeń bezpieczeństwa informacji, skutków naruszenia zasad bezpieczeństwa informacji, odpowiedzialności prawnej oraz stosowania środków zapewniających bezpieczeństwo informacji, z uwzględnieniem urządzeń i oprogramowania minimalizującego ryzyko błędów ludzkich, jest też istotnym elementem SZBI. Pracownik, jako część każdego systemu zarządczego wymaga szczególnego podejścia i zapewnienia ciągłego rozwoju poprzez system szkoleń. Ważnym elementem, w szczególności z uwagi na zmieniające się zagrożenia bezpieczeństwa informacji i zmieniające się zabezpieczenia, jest ich cykliczność.

Analiza zebranego materiału dowodowego sprzeciwia się przyjęciu, że WUOZ zapewnia szkolenia osób zaangażowanych w proces przetwarzania informacji w zakresie, o którym stanowi § 20 ust. 2 pkt 6 lit. a-c r.k.r.i. Zagadnienie ocenione zostało zatem **pozytywnie z nieprawidłowościami.**

Na podstawie ustaleń kontroli, w celu dalszego usprawnienia realizacji kontrolowanego zadania należy:

1. Zamieścić na stronie podmiotowej BIP informacje o adresie elektronicznej skrzynki podawczej - w formie identyfikatora URI oraz o wymaganiach określonych przepisami prawa dotyczących doręczania dokumentów elektronicznych, zgodnie z obowiązkiem wynikającym z § 3 ust. 1 Rozporządzenia Prezesa Rady Ministrów z dnia 14 września 2011 r. w sprawie sporządzania i doręczania dokumentów elektronicznych oraz udostępniania formularzy, wzorów i kopii dokumentów elektronicznych.

2. Zapewnić odpowiedni poziom dokładności i złożoności dokumentacji SZBI w zakresie bezpieczeństwa informacji oraz poddawać ją regularnym przeglądom (§ 20 ust. 1 r.k.r.i).
3. Przeprowadzać analizę ryzyka, rzetelnie ją dokumentować i zapoznawać z jej treścią kierownictwo WUOZ we Wrocławiu.
4. Ujednolicić procedury zgłaszania incydentów określone w SZBI, wprowadzić rejestr incydentów służący ich identyfikacji.
5. Wyznaczyć zespół audytorów wewnętrznych i przeprowadzać audyt wewnętrzny nie rzadziej niż raz w roku, zgodnie z § 20 ust. 2 pkt 14 r.k.r.i.
6. Ujednolicić treść Regulaminu Pracy Zdalnej w WUOZ z Zarządzeniem 39/2019 wprowadzającym Politykę Bezpieczeństwa Informacji i Systemów Teleinformatycznych w zakresie standardu hasła zawierającego 8 znaków (duże+małe litery+cyfry+min. znak specjalny).
7. Sformalizować zasady wykonywania, przechowywania i testowania kopii zapasowych danych i systemów, aby zapewnić wypełnienie normy § 20 ust. 2 pkt 12 lit. b) i e) r.k.r.i.
8. Wykonywać inwentaryzację sprzętu i oprogramowania służącego do przetwarzania informacji, obejmującej ich rodzaj i konfigurację, w celu wypełnienia dyspozycji przepisu § 20 ust. 2 pkt 2 rozporządzenia KRI.
9. Zapewnić, aby zawierane umowy serwisowe ze stronami trzecimi zawierały zapisy gwarantujące odpowiedni poziom bezpieczeństwa informacji w trakcie realizacji umowy, zgodnie z obowiązkiem wynikającym z § 20 ust. 2 pkt 10 rozporządzenia KRI.
10. Zapewnić regularne szkolenia pracowników zaangażowanych w proces przetwarzania informacji, z uwzględnieniem zagadnień wynikających z § 20 ust. 2 pkt 6 lit. a-c rozporządzenia KRI.

Na podstawie art. 46 ust. 3 pkt 3 ustawy o kontroli w administracji rządowej proszę o przekazanie **w terminie do dnia 19 października 2023 r.** o informacji o wykonaniu zaleceń i wykorzystaniu wniosków, a także o podjętych działaniach mających na celu wyeliminowanie stwierdzonych nieprawidłowości.

Z up. WOJEWODY DOLNOŚLĄSKIEGO
II WICEWOJEWODA DOLNOŚLĄSKI
Bogusław Szpytma