Zachodniopomorski
Urząd Wojewódzki

K-2.1611.1.2024.5.IO
Szczecin, 14.02.2025 r.

WYSTĄPIENIE POKONTROLNE

Przedmiot kontroli	Bezpieczeństwo teleinformatyczne w administracji rządowej i ochrona danych osobowych.
Nazwa i adres organu kontrolującego	Wojewoda Zachodniopomorski, ul. Wały Chrobrego 4, 70-502 Szczecin.
Nazwa i adres organu kontrolowanego	Zachodniopomorski Komendant Wojewódzki Państwowej Straży Pożarnej, ul. Firlika 9-14, 71-637 Szczecin.
Osoba pełniąca funkcję Zachodniopomorskiego Komendanta Wojewódzkiego Państwowej Straży Pożarnej w okresie objętym kontrolą	Nadbrygadier Jarosław Tomczyk do 12 stycznia 2024 r. Starszy brygadier Mirosław Pender od 13 stycznia 2024 r.
Okres objęty kontrolą	od dnia 1 stycznia 2021 r. do dnia 15 marca 2024 r.
Kontrolerzy	Pracownicy Zachodniopomorskiego Urzędu Wojewódzkiego w Szczecinie: - Pan Jan Kępiński – radca generalny w Biurze Organizacji i Kadr, - Pani Iwona Olesińska – główny specjalista w Wydziale Kontroli.
Nr upoważnienia	Nr 15/24 z dnia 23 lutego 2024 r.
Podstawy prawne do przeprowadzenia kontroli	- art. 6 ust. 4 pkt 1 w związku z art. 16 ust. 1 i 2 ustawy z dnia 15 lipca 2011 r. o kontroli w administracji rządowej (Dz. U. z 2020 r., poz. 224), - art. 28 ust. 1 pkt 1 ustawy z dnia 23 stycznia 2009 r. o wojewodzie i administracji rządowej w województwie (Dz. U. z 2023r., poz. 190).
Kryteria prowadzenia kontroli	legalność, rzetelność
Rodzaj kontroli i tryb kontroli	kontrola planowa, tryb zwykły
Termin kontroli	4-15 marca 2024 r.
Osoby udzielające wyjaśnień w trakcie kontroli	XXX Naczelnik Wydziału Bezpieczeństwa Informacji, XXX Inspektor Ochrony Danych[1].

[1] Inspektor Ochrony Danych - dalej IOD.

Obszar kontroli Nr 1	Prawidłowość działania i bezpieczeństwo systemów teleinformatycznych wykorzystywanych do realizacji zadań publicznych.
Podstawa prawna	Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych[2].

1.1 Dokumenty z zakresu bezpieczeństwa informacji. Zaangażowanie kierownictwa podmiotu.

Podstawa prawna: § 19 ust. 1 rozporządzenia 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 pkt 1 rozporządzenia KRI:** *Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienie (...) aktualizacji regulacji wewnętrznych w zakresie dotyczącym zmieniającego się otoczenia;* **§ 19 ust. 3 rozporządzenia KRI:** *Wymagania określone w ust. 1 i 2 uznaje się za spełnione, jeżeli system zarządzania bezpieczeństwem informacji został opracowany na podstawie Polskiej Normy PN-ISO/IEC 27001, a ustanawianie zabezpieczeń, zarządzanie ryzykiem oraz audytowanie odbywa się na podstawie Polskich Norm związanych z tą normą.*

Ustalenia kontroli

Wymagania dotyczące systemów teleinformatycznych, w których przetwarzane są rejestry publiczne w postaci teleinformatycznej określone zostały w § 19 ust. 1 rozporządzenia KRI. Zgodnie z tym przepisem, podmiot realizujący zadania publiczne ma obowiązek opracowania i ustanowienia, wdrożenia i eksploatowania, monitorowania i przeglądania oraz utrzymania i doskonalenia systemu bezpieczeństwa informacji zapewniającego poufność, dostępność, integralność informacji.

W Komendzie Wojewódzkiej Państwowej Straży Pożarnej w Szczecinie[3] w okresie objętym kontrolą obowiązywały następujące dokumenty z zakresu bezpieczeństwa informacji:

- *Polityka ochrony danych osobowych w Komendzie Wojewódzkiej Państwowej Straży Pożarnej w Szczecinie, maj 2018r.;*
- *Zarządzenie Nr 11/2024 Zachodniopomorskiego Komendanta Wojewódzkiego Państwowej Straży Pożarnej w Szczecinie z dnia 12 lutego 2024 r. w sprawie wprowadzenia polityki bezpieczeństwa teleinformatycznego w Komendzie Wojewódzkiej PSP w Szczecinie*.

W wyniku analizy dokumentacji związanej z bezpieczeństwem informacji stwierdzono, że funkcjonujące w Jednostce procedury spełniają wymogi określone w § 19 ust. 2 pkt 1 rozporządzenia KRI w zakresie bezpieczeństwa informacji. Procedury zawierają między innymi definicję bezpieczeństwa informacji, oświadczenie o zaangażowaniu kierownictwa w zarządzanie bezpieczeństwem informacji; wyjaśnienie zasad, norm i wymagań zgodności mających szczególne znaczenie dla organizacji; definicje ogólnych i szczególnych obowiązków w odniesieniu do zarządzania bezpieczeństwem informacji.

[2] Rozporządzenie Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U. 2024 poz. 773), zwane dalej „rozporządzeniem KRI".

[3] Komenda Wojewódzka Państwowej Straży Pożarnej w Szczecinie- dalej *Komenda Wojewódzka PSP lub KW PSP.*

W Komendzie Wojewódzkiej Państwowej Straży Pożarnej w Szczecinie wdrożono procedury dotyczące zarządzania bezpieczeństwem informacji zapewniające poufność, dostępność i integralność informacji z uwzględnieniem takich atrybutów, jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność działań.

(dowód: akta kontroli str. 25-50; 120-169)

1.2 Analiza zagrożeń związanych z przetwarzaniem informacji.
Podstawa prawna: § 19 ust. 2 pkt 3 rozporządzenia KRI: *Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez: przeprowadzanie okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji oraz podejmowania działań minimalizujących to ryzyko, stosownie do wyników przeprowadzonej analizy.*

Ustalenia kontroli
Analiza ryzyka, obejmująca wszystkie aktywa Jednostki oraz odpowiednie i pogłębione szacowanie zidentyfikowanych ryzyk jest jednym z najistotniejszych elementów zarządzania bezpieczeństwem informacji, pozwalającym na zastosowanie odpowiednich mechanizmów przeciwdziałania w sytuacji materializacji ryzyk. Procedura szacowania ryzyka powinna być przeprowadzana okresowo, jednak zawsze w przypadku pojawienia się nowych zagrożeń, co wynika z faktu, że rodzaj i poziom zastosowanych zabezpieczeń jest względny i jest zależny od istotności informacji podlegających ochronie.
Kontrolującym przedstawiono *Notatkę Służbową*, sporządzoną 26 lutego 2024r., której integralną częścią jest *Analiza ryzyka systemów teleinformatycznych użytkowanych w KW PSP*. Analiza ryzyka została sporządzona w oparciu o wytyczne Komendy Głównej PSP dotyczące szacowania ryzyka, ujęte w *Metodyce szacowania ryzyka naruszenia praw lub wolności osób fizycznych w Państwowej Straży Pożarnej.* W dokumencie określono zagrożenia dla wskazanych zasobów, źródła tych zagrożeń oraz prawdopodobieństwo i skutki wpływu zdarzeń na czynniki decydujące o bezpieczeństwie danych.
Stwierdzono, że wyżej przywołana analiza ryzyka, obejmująca zidentyfikowane aktywa Jednostki, wypełnia dyspozycję, o której mowa w § 19 ust. 2 pkt 3 rozporządzenia KRI, W Jednostce powstał i został zatwierdzony *Plan ciągłości działania na wypadek awarii lub innego czynnika zewnętrznego powodującego brak dostępności do systemu teleinformatycznego oraz metodologię odtwarzania systemów teleinformatycznych po ich awarii w KW PSP w Szczecinie*.

(dowód: akta kontroli str. 170-182, 264-271, 460-463, 484-490)

1.3 Inwentaryzacja sprzętu i oprogramowania informatycznego.
Podstawa prawna: § 19 ust. 2 pkt 2 rozporządzenia KRI: *Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez: utrzymanie aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji obejmującej ich rodzaj i konfigurację.*

Ustalenia kontroli
Zgodne z § 19 ust. 2 pkt 2 rozporządzenia KRI zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez utrzymywanie aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji obejmującej ich rodzaj i konfigurację. Ponadto wszystkie aktywa informatyczne powinny być zidentyfikowane oraz powinien być sporządzany i aktualizowany ich spis. Inwentaryzacja m.in. sprzętu informatycznego powinna zawierać informację o jego rodzaju i konfiguracji, przez co możliwe będzie jego odtworzenie po katastrofie lub innym zdarzeniu losowym.

Kontrolującym przedstawiono rejestr komputerów, urządzeń i oprogramowania służącego do przetwarzania informacji. Ustalono, że okazana ewidencja zawierała między innymi informacje o rodzaju użytkowanego w Jednostce sprzętu (nazwie i jego charakterystyce), nazwie oraz wersji systemu operacyjnego, nazwie procesora, zainstalowanym oprogramowaniu, pojemności pamięci oraz współpracujących urządzeniach peryferyjnych.
Mając na uwadze powyższe stwierdzono, że w Komendzie Wojewódzkiej PSP prowadzona jest inwentaryzacja sprzętu i oprogramowania, zgodnie z wymogami rozporządzenia KRI. (dowód: akta kontroli str. 491-493)

1.4 Zarządzanie uprawnieniami do pracy w systemach informatycznych.
Podstawa prawna: § 19 ust. 2 pkt 4 rozporządzenia 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 rozporządzenia KRI:** *Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez: zapewnienie bezzwłocznej zmiany uprawnień, w przypadku zmiany zadań osób, o których mowa w pkt 4.*

Ustalenia kontroli
Przepisy § 19 ust. 2 pkt 4 i pkt 5 rozporządzenia KRI stanowią m.in, że kierownictwo podmiotu publicznego w celu zapewnienia bezpieczeństwa informacji powinno podjąć działania zapewniające, że osoby zaangażowane w proces przetwarzania informacji posiadają stosowne uprawnienia, adekwatne do realizowanych zadań, a także podjąć bezzwłoczne działania w przypadku zmiany zadań tych osób. Przetwarzanie informacji w systemach teleinformatycznych wymaga dostępu do danych przez uprawnione osoby, w ustalonym zakresie.
Kwestie nadawania i odbierania uprawnień do pracy w systemie informatycznym uregulowano w *Polityce Bezpieczeństwa Teleinformatycznego w KW PSP w Szczecinie* w postaci procedury nadawania i odbierania uprawnień do przetwarzania informacji. Zgodnie z regulacjami przyjętymi w Jednostce nadawanie uprawnień do przetwarzania informacji oraz uprawnień dotyczących dostępu do systemu informatycznego odbywa się na pisemny wniosek Kierownika komórki organizacyjnej. Po akceptacji Komendanta Wojewódzkiego PSP Administrator Systemów Informatycznych nadaje uprawnienia do systemów wskazanych we wniosku. Administrator Systemów prowadzi rejestr, w którym odnotowuje czynności związane z nadawaniem, odbieraniem i weryfikacją uprawnień przyznanych użytkownikom systemów teleinformatycznych.
Kontrolującym przedstawiono:

- *wnioski o dostęp do usług i systemów teleinformatycznych;*
- *wnioski o dostęp do Systemów Centralnych PSP*;
- *upoważnienia do przetwarzania danych osobowych*. Dokument upoważnienia określa jego obszar - wynikający z zadań pracownika realizowanych na zajmowanym stanowisku;
- oświadczenie, w których zawarto między innymi zobowiązanie pracownika do zachowania w tajemnicy przetwarzanych danych osobowych. W dokumencie nie wskazano czasu trwania tego zobowiązania. Kontrolujący sugerują, by zrewidować powyższy dokument pod kątem wskazania okresu obowiązywania zobowiązania, rozszerzając go na okres po ustaniu stosunku pracy.

W trakcie kontroli dokonano sprawdzenia odbierania uprawnień dostępu do systemów informatycznych dziewięciu pracownikom, z którymi rozwiązano stosunek pracy. Nie stwierdzono nieprawidłowości polegających na niezachowaniu wymogu bezzwłocznego odebrania uprawnień w systemach informatycznych.

(dowód: akta kontroli str. 31-32, 402-433, 547-597)

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

Ustalenia kontroli
Z analizy przedłożonej dokumentacji oraz złożonych przez IOD wyjaśnień wynika, że zakres tematyczny szkoleń przeprowadzonych w KW PSP nie obejmował wszystkich zagadnień wskazanych w § 19 ust. 2 pkt 6 rozporządzenia KRI.
Szkolenia, których celem jest zagwarantowanie bezpieczeństwa w zakresie przetwarzania informacji, ze względu na zmieniające się zagrożenia związane z dynamicznym rozwojem technologii informatycznych winny mieć charakter cykliczny i obejmować wszystkie zagadnienia wskazane w § 19 ust. 2 pkt 6 rozporządzenia KRI.

(dowód: akta kontroli str. 451-459)

1.6 Procedury zgłaszania incydentów naruszenia bezpieczeństwa informacji.
Podstawa prawna: § 19 ust. 2 pkt 13 rozporządzenia 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.*

Ustalenia kontroli
Kwestie związane z obsługą incydentów naruszenia bezpieczeństwa danych osobowych w KW PSP uregulowano w *Polityce ochrony danych osobowych w Komendzie Wojewódzkiej Państwowej Straży Pożarnej w Szczecinie*, w postaci *Instrukcji postępowania w sytuacji naruszenia ochrony danych osobowych*. W dokumencie określono sposób postępowania w przypadku stwierdzenia naruszenia danych osobowych, wskazując jednocześnie osoby odpowiedzialne za realizację odpowiednich działań. Zgodnie z wyjaśnieniami IOD w okresie objętym kontrolą nie odnotowano incydentów naruszenia *ochrony danych osobowych*. Kontrolującym przedstawiono *Rejestry incydentów bezpieczeństwa i działań korygujących i zapobiegawczych* z lat objętych kontrolą, które nie zawierają wpisów.
Zgodnie z § 19 ust. 2 pkt 13 rozporządzenia KRI *zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez: bezzwłoczne zgłaszanie incydentów naruszenia bezpieczeństwa informacji (...)*, wobec czego elementy systemu zarządzania bezpieczeństwem informacji powinny obejmować bezpieczeństwo informacji w całej organizacji i nie ograniczać się do ochrony danych osobowych. Stwierdzono, że procedura obowiązująca w KW PSP w tym zakresie częściowo wypełnia dyspozycję przywołanego powyżej rozporządzenia KRI.

(dowód: akta kontroli str. 161-164)

1.7 Audyt wewnętrzny z zakresu bezpieczeństwa informacji.
Podstawa prawna: § 19 ust. 2 pkt 14 rozporządzenia KRI: *Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez: zapewnienie okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji, nie rzadziej niż raz na rok.*

Ustalenia kontroli
W latach 2021-2023 w Komendzie Wojewódzkiej PSP nie przeprowadzono audytów wewnętrznych w zakresie bezpieczeństwa informacji.
Nieprzeprowadzanie audytu wewnętrznego może wpływać na ocenę skuteczności przyjętych w Jednostce rozwiązań w zakresie bezpieczeństwa informacji; audyt wewnętrzny stanowi bowiem istotne źródło informacji dla kierownictwa Jednostki o realnym stanie bezpieczeństwa, różnych aspektach jego utrzymania oraz wskazuje obszary wymagające podjęcia działań korygujących.
Mając na względzie powyższe, należy stwierdzić, że w okresie objętym kontrolą nie zrealizowano w Jednostce dyspozycji, o której mowa w § 19 ust. 2 pkt 14 rozporządzenia KRI.

1.8 Kopie zapasowe.
Podstawa prawna: § 19 ust. 2 pkt 12 lit. b, e rozporządzenia KRI: *Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez: minimalizowanie ryzyka utraty informacji w wyniku awarii, zapewnieniu bezpieczeństwa plików systemowych.*

Ustalenia kontroli
Zgodnie z wymogami określonymi w § 19 ust. 2 pkt 12 lit. b) i e) rozporządzenia KRI, zarządzanie bezpieczeństwem informacji realizowane jest w szczególności poprzez zapewnienie przez kierownictwo podmiotu publicznego warunków umożliwiających realizację i egzekwowanie m.in. odpowiedniego poziomu bezpieczeństwa w systemach teleinformatycznych, polegającego w szczególności na minimalizowaniu ryzyka utraty informacji w wyniku awarii i zapewnieniu bezpieczeństwa plików systemowych.
Zasady, harmonogram tworzenia kopii zapasowych zbiorów danych oraz kwestie przechowywania nośników kopii zapasowych uregulowane zostały w *Polityce Bezpieczeństwa Teleinformatycznego w KW PSP w Szczecinie.*
Stwierdzono, że w Jednostce zgodnie z procedurą wykonuje się i przechowuje kopie zapasowe użytkowanych systemów.
Z wyjaśnień Naczelnika Wydziału Bezpieczeństwa Informacji wynika również, że realizowane jest próbne testowanie w celu sprawdzenia poprawności wykonania kopii bezpieczeństwa.

(dowód: akta kontroli str. 45-47)

1.9 Wdrożone i wykorzystywane rozwiązania organizacyjne i techniczne zapewniające bezpieczeństwo informacji.
Podstawa prawna: § 15 ust. 1 rozporządzenia KRI: *Systemy teleinformatyczne używane przez podmioty realizujące zadania publiczne projektuje się, wdraża oraz eksploatuje z uwzględnieniem ich funkcjonalności, niezawodności, używalności, wydajności przenoszalności i pielęgnowalności, przy zastosowaniu norm oraz uznanych w obrocie profesjonalnym standardów i metodyk;* **§ 19 ust. 2 rozporządzenia KRI:** *Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez:* **pkt 7:** *zapewnienie ochrony przetwarzania 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, modyfikację, usunięcie lub zniszczenie;* **pkt 11:** *ustalenie zasad postępowania z informacjami, zapewniających minimalizację wystąpienia ryzyka kradzieży informacji i środków przetwarzania informacji, w tym urządzeń mobilnych;* **§ 19 ust. 2 pkt 12 rozporządzenia 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, 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;* **§ 19 ust. 4 rozporządzenia KRI:** *Niezależnie od zapewnienia działań, o których mowa w ust. 2, w przypadkach uzasadnionych analizą ryzyka w systemach teleinformatycznych podmiotów realizujących zadania publiczne należy ustanowić dodatkowe zabezpieczenia.*

Ustalenia kontroli
W celu ustanowienia zabezpieczeń uniemożliwiających osobom nieuprawnionym modyfikację, usunięcie lub zniszczenie informacji każdemu pracownikowi KW PSP nadano identyfikator i hasło wejścia do systemów zainstalowanych na komputerach użytkowników oraz do programów, z których korzystają. Złożoność hasła była zgodna z wymogami rozporządzenia w sprawie dokumentacji i warunków technicznych.
W wyniku oględzin ośmiu stanowisk pracy, przeprowadzonych w toku czynności kontrolnych ustalono, że:

- na każdym urządzeniu dostęp do systemu operacyjnego możliwy był jedynie po wprowadzeniu nazwy użytkownika i hasła,
- komputery miały zainstalowane oprogramowanie antywirusowe,
- na wszystkich jednostkach skonfigurowano wygaszacz ekranu,
- ustawienie monitorów kontrolowanych stanowisk pracy uniemożliwia odczyt wyświetlanych danych przez osoby postronne,
- żadnemu z użytkowników nie nadano uprawnień administratora uniemożliwiając w ten sposób instalowanie oprogramowania niewiadomego pochodzenia lub zmianę ustawień systemu operacyjnego a także ingerencję w rejestry zdarzeń.

Ponadto stwierdzono, że:

- sieć informatyczną Jednostki zabezpieczono przy wykorzystaniu zapory sieciowej firewall,
- wszystkie stanowiska w KW PSP są podłączone do zasilacza awaryjnego UPS,
- w budynku zainstalowano monitoring wizyjny.

(dowód: akta kontroli str. 509-510)

1.10 Rozliczalność działań w systemach teleinformatycznych.
Podstawa prawna: § 20 ust. 2 rozporządzenia 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 rozporządzenia 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 rozporządzenia 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.*

Ustalenia kontroli

Przetwarzanie informacji w systemach teleinformatycznych wymaga dostępu do danych przez uprawnione osoby i obiekty systemowe (procesy) w ustalonym zakresie. Zapewnienie rozliczalności operacji polega na gromadzeniu informacji o tym, kto, kiedy i jakie czynności wykonał w systemie teleinformatycznym. Obligatoryjnie podlegają dokumentowaniu w postaci zapisów w dziennikach systemów (logi) wszelkie działania dostępu do systemu teleinformatycznego z uprawnieniami administracyjnymi, w zakresie konfiguracji systemu i jego zabezpieczeń a także działania, gdy przetwarzanie danych podlega prawnej ochronie (np. zgodnie z ustawą o ochronie danych osobowych).

Zgodnie z wyjaśnieniami Naczelnika Wydziału Bezpieczeństwa Informacji z 8 marca 2024 r. logi systemowe zapisywane są dla modułu finansowego Rozrachunki Premium programu Progman. Natomiast dla modułu Finanse Premium taka funkcjonalność będzie dostępna w kolejnej wersji programu. Pozostałe programy finansowe nie posiadają funkcjonalności w postaci zapisu logów. Ze złożonych wyjaśnień wynika również, że *w module Rozrachunki Premium logi systemowe są trzymane przez 6 dni*.

Brak zapisów w logach systemu narusza § 20 ust. 2 rozporządzenia KRI, stanowiącego, że *w dziennikach systemów odnotowuje się obligatoryjnie działania użytkowników (...) polegające na dostępie do systemu z uprawnieniami administracyjnymi(...)* oraz *do przetwarzanych w systemach danych podlegających prawnej ochronie w zakresie wymaganym przepisami prawa.* Logi systemu winny być przechowywane przez okres ponad 2 lat, wobec czego w tym zakresie nie wypełniono dyspozycji § 20 ust. 4 wyżej opisanego rozporządzenia.

Zgodnie z wyjaśnieniami Naczelnika Wydziału Bezpieczeństwa Informacji prowadzone są działania związane z analizą logów eksploatowanych systemów, w celu identyfikacji działań niepożądanych.

dowód: akta kontroli str. 464-472)

Stwierdzone uchybienia / nieprawidłowości w obszarze Nr 1	• Nieprzeprowadzenie w latach 2021 - 2023 audytów wewnętrznych obejmujących zagadnienia związane z bezpieczeństwem informacji, do czego zobowiązuje zapis § 19 ust. 2 pkt 14 rozporządzenia KRI. • Zakres tematyczny szkoleń przeprowadzonych w KW PSP nie obejmował wszystkich zagadnień wskazanych w § 19 ust. 2 pkt 6 rozporządzenia KRI. • Zawężenie procedur dotyczących incydentów naruszenia bezpieczeństwa informacji do naruszeń ochrony danych osobowych.

	• Nieodnotowywanie w dziennikach systemów opisanych w punkcie 1.10 działań użytkowników z uprawnieniami administracyjnymi, co nie wypełnia dyspozycji § 20 ust. 2 rozporządzenia KRI. • Logi systemów opisanych w punkcie 1.10 nie są przechowywane przez okres 2 lat od dnia ich zapisu, co jest niezgodne z zapisami § 20 ust. 4 rozporządzenia KRI.
Ocena obszaru kontroli	Zakresy kontroli opisane w pkt 1-4 oraz 8-9 oceniono **pozytywnie**. Zagadnienia ujęte w pkt 5-6, 10 w związku ze stwierdzonymi odstępstwami od obowiązujących uregulowań oceniono **pozytywnie z nieprawidłowościami.** Mając natomiast na względzie wagę stwierdzonych nieprawidłowości opisanych w pkt 7, polegających na nieprzeprowadzaniu corocznych audytów wewnętrznych z zakresu bezpieczeństwa informacji, do czego zobowiązują zapisy § 19 ust. 2 pkt 14 rozporządzenia KRI, wskazany zakres oceniono **negatywnie.**

Obszar kontroli Nr 2	Ochrona danych osobowych.
Podstawa prawna	Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)[4].

2.1 Wyznaczenie IOD.

Ustalenia kontroli

Formalne zgłoszenie IOD do UODO[5] w oparciu o zapisy ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych nastąpiło 5 lipca 2018 r. Zgłoszenia dokonano w terminie wskazanym właściwymi przepisami prawa.

Zgodnie z dyspozycją art. 37 ust. 7 rozporządzenia RODO oraz art. 11 Ustawy o ochronie danych osobowych dane Inspektora Ochrony Danych; sposób i formę kontaktu z IOD zawarto w klauzuli informacyjnej zamieszczonej na stronie www pod adresem https://www.gov.pl/web/kwpsp-szczecin/rodo. Stwierdzono, że na dzień rozpoczęcia czynności kontrolnych powyższe dane były aktualne, a osoba wyznaczona do pełnienia funkcji Inspektora Ochrony Danych spełniała wymogi określone w art. 37 ust. 5 rozporządzenia RODO w zakresie kwalifikacji zawodowych.

(dowód: akta kontroli str. 436-437)

2.2 Rejestr czynności przetwarzania[6].

Rejestr czynności przetwarzania jest uporządkowanym zbiorem informacji o procesach przetwarzania danych, jakie winny być prowadzone w organizacji. Zakres wymaganych

[4] Zwane dalej rozporządzeniem RODO, Dz. Urz. UE L2016.119.
[5] UODO - Urząd Ochrony Danych Osobowych.
[6] Rejestr czynności przetwarzania – dalej RCP.

informacji wskazano w art. 30 ust. 1 rozporządzenia RODO. RCP jest dokumentem, w którym organizacja zapisuje informacje o tym, w jaki sposób (jako administrator) przetwarza dane osobowe.

Ustalenia kontroli
W KW PSP utworzono rejestr czynności przetwarzania danych osobowych. Rejestr prowadzony jest w formie elektronicznej oraz zawiera elementy określone w art. 30 ust. 1 rozporządzenia RODO. Według stanu na 21 marca 2024 r. rejestr czynności przetwarzania liczył 75 pozycji (celów przetwarzania).

(dowód: akta kontroli str. 184-191)

2.3 Rejestr kategorii czynności przetwarzania.

Zgodnie z definicją wskazaną w art. 4 rozporządzenia RODO, podmiotem przetwarzającym jest osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który przetwarza dane osobowe w imieniu administratora.
Zgodnie z art. 30 ust. 2 rozporządzenia RODO, każdy z tych podmiotów ma obowiązek prowadzenia rejestru kategorii czynności przetwarzania dokonywanych w imieniu administratora. Wyżej przywołany artykuł rozporządzenia RODO wskazuje wymagane elementy tego rejestru oraz warunki jego prowadzenia.

Ustalenia kontroli
W KW PSP utworzono Rejestr kategorii czynności przetwarzania danych osobowych. Rejestr prowadzony jest w formie elektronicznej oraz zawiera elementy określone w art. 30 ust. 2 rozporządzenia RODO.

(dowód: akta kontroli str. 183)

2.4 Rejestr incydentów.

Zgodnie z wymaganiami art. 33 ust. 5 rozporządzenia RODO *Administrator dokumentuje wszelkie naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze. Dokumentacja ta musi pozwolić organowi nadzorczemu weryfikowanie przestrzegania niniejszego artykułu.* Administrator winien rejestrować informacje o naruszeniu ochrony danych osobowych obejmujące okoliczności naruszenia, przebieg i informacje dotyczące naruszonych danych osobowych. Ewidencja powinna obejmować ponadto skutki i konsekwencje naruszenia oraz działania naprawcze podjęte przez administratora. Prowadzenie ewidencji łączy się z zasadą rozliczalności przewidzianą w art. 5 ust. 2 rozporządzenia RODO oraz obowiązkami administratora wynikającymi z art. 24 rozporządzenia RODO. Grupa Robocza Art. 29[7] wskazuje ponadto, że w przypadku podjęcia decyzji o niezgłoszeniu naruszenia, wskazane jest udokumentowanie takiego faktu w ewidencji wraz z podaniem przyczyny, dla której administrator uznaje ryzyko naruszenia praw i wolności osób fizycznych za mało prawdopodobne.

Ustalenia kontroli
W KW PSP utworzono rejestr incydentów. Na dzień przeprowadzenia kontroli IOD wyjaśnił, że w Jednostce, w badanym okresie nie odnotowano naruszeń danych osobowych. Rejestr zawiera następujące pozycje: l.p. incydentu, osoba zgłaszająca

[7] Grupa robocza ds. ochrony osób fizycznych w zakresie przetwarzania danych osobowych, zwana Grupą Roboczą, powołana została na mocy art. 29 Dyrektywy 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych jako niezależny podmiot o charakterze doradczym. Grupa ta została rozwiązana 25 maja 2018 roku a w jej miejsce została powołana Europejska Rada Ochrony Danych.

okoliczności naruszenia danych osobowych, przebieg i naruszone dane osobowe, czynności związane z obsługą incydentu, skutki i konsekwencje naruszenia, działania naprawcze podjęte przez administratora, data zakończenia obsługi incydentu.

(dowód: akta kontroli str. 451)

2.5 Analiza ryzyka.

Ustalenia kontroli

W KW PSP, w badanym okresie przeprowadzono analizę ryzyka w zakresie ochrony danych osobowych. Kontrolującym przedstawiono:

- Analizę ryzyka w zakresie ochrony osobowych w postaci macierzy z przypisanymi wartościami,
- *Metodykę szacowania ryzyka naruszenia praw lub wolności osób fizycznych w Państwowej Straży Pożarnej*,
- *Szacowanie i analiza ryzyka naruszenia praw i wolności osób fizycznych związanego z przetwarzaniem danych osobowych w systemie monitoringu wizyjnego Komendy Wojewódzkiej PSP w Szczecinie.*

(dowód: akta kontroli str. 170-182, 494-507)

2.6 Klauzula informacyjna.

Ustalenia kontroli

Na stronie internetowej KW PSP umieszczono informację skierowaną do klientów i stron zainteresowanych o celu, zakresie i kategoriach przetwarzania danych osobowych; czasie przetwarzania danych oraz o przysługujących prawach zgodnie z rozporządzeniem RODO. Wskazano Administratora danych oraz podano kontakt do Inspektora Ochrony Danych. W Jednostce funkcjonuje również klauzula informacyjna dedykowana pracownikom oraz klauzula dotyczącą monitoringu obiektów.

(dowód: akta kontroli str. 197)

2.7 Umowy powierzenia przetwarzania danych osobowych.

Ustalenia kontroli

Zgodnie z art. 28 ust. 3 i ust. 9 rozporządzenia RODO, w badanym okresie KW PSP zawarła następujące umowy powierzenia przetwarzania danych osobowych XXX. Umowy zawierały wszystkie elementy wymagane dyspozycją art. 28 ww. rozporządzenia, między innymi: przedmiot i czas trwania przetwarzania, charakter i cel przetwarzania, rodzaj danych osobowych, obowiązki i prawa administratora. Podmioty przetwarzające zobowiązano do przechowywania danych zgodnie z umową i rozporządzeniem RODO oraz zachowania w tajemnicy danych osobowych i innych informacji pozyskanych w trakcie realizacji umowy.

(dowód: akta kontroli str. 272-401)

Stwierdzone nieprawidłowości w obszarze Nr 2	**nie stwierdzono nieprawidłowości**
Ocena obszaru kontroli	**Pozytywna**

	Obszar kontroli: **Nr 1. Prawidłowość działania i bezpieczeństwo systemów teleinformatycznych wykorzystywanych do realizacji zadań publicznych:**

Zalecenia	• Przeprowadzać co roku audyt wewnętrzny z zakresu bezpieczeństwa informacji, do czego zobowiązują zapisy § 19 ust. 2 pkt 14 rozporządzenia KRI. • Przeprowadzać szkolenia z zakresu bezpieczeństwa informacji obejmujące wszystkie zagadnienia wskazane w § 19 ust. 2 pkt 6 rozporządzenia KRI. • Uzupełnić procedury dotyczące postępowania w przypadku naruszenia ochrony danych osobowych o pozostałe obszary, w których mogą wystąpić przypadki naruszenia bezpieczeństwa przetwarzanych w Jednostce informacji, zgodne z dyspozycją § 19 ust. 2 pkt 13 rozporządzenia KRI. • Odnotowywać w dziennikach systemów opisanych w punkcie 1.10 działania użytkowników z uprawnieniami administracyjnymi, zgodnie z dyspozycją § 20 ust. 2 rozporządzenia KRI. • Przechowywać logi systemów opisanych w punkcie 1.10 przez okres 2 lat od dnia ich zapisu, zgodne z dyspozycją § 20 ust. 4 rozporządzenia KRI. **Nr 2. Ochrona danych osobowych:** w związku z brakiem nieprawidłowości nie sformułowano zaleceń.
Pouczenia	– zgodnie z art. 48 ustawy z dnia 15 lipca 2011 roku o kontroli w administracji rządowej (Dz.U. z 2020 r. poz. 224) od wystąpienia pokontrolnego nie przysługują środki odwoławcze, – o podjętych działaniach, mających na celu realizację zaleceń pokontrolnych, proszę poinformować mnie za pośrednictwem Wydziału Kontroli Zachodniopomorskiego Urzędu Wojewódzkiego w Szczecinie w terminie 14 dni od daty otrzymania niniejszego wystąpienia.
Podpis kierownika jednostki kontrolującej	Z upoważnienia Wojewody Zachodniopomorskiego Bartosz Brożyński I Wicewojewoda Zachodniopomorski */podpisano kwalifikowanym podpisem elektronicznym/*