WOJEWODA
ZACHODNIOPOMORSKI

Szczecin, dnia 07 sierpnia 2023 r.

K-2.1611.1.2023.8.IO

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 Wojewódzki Inspektor Nadzoru Budowlanego ul. Wały Chrobrego 4, 70-502 Szczecin
Osoba pełniąca funkcję organu w okresie prowadzenia kontroli oraz w okresie objętym kontrolą	Pan Ryszard Kabat
Okres objęty kontrolą	Od 1 stycznia 2020 r. do dnia 24 marca 2023 r.
Kontrolujący	Pracownicy Zachodniopomorskiego Urzędu Wojewódzkiego w Szczecinie*:* - Pan Jan Kępiński – radca generalny w Biurze Organizacji i Kadr, - Pani Iwona Olesińska – główny specjalista* w Wydziale Kontroli. *Kontroler w okresie prowadzenia kontroli zajmował stanowisko starszego inspektora wojewódzkiego
Nr upoważnienia	Nr 15/23 z dnia 1 marca 2023 r. oraz Nr 15/2/23 z dnia 17 marca 2023r.
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
Termin kontroli	6-24 marca 2023 r.
Rodzaj i tryb kontroli	kontrola planowa, tryb zwykły
Osoby udzielające wyjaśnień w trakcie kontroli	- Pan Ryszard Kabat – Zachodniopomorski Wojewódzki Inspektor Nadzoru Budowlanego, - Pan Kazimierz Hen – zastępca Zachodniopomorskiego Wojewódzkiego Inspektora Nadzoru Budowlanego,

	- Pan Andrzej Nowicki- Administrator systemu, - Pani Iwona Białowąs - Inspektor Ochrony Danych[1].
Obszar nr 1. Prawidłowość działania i bezpieczeństwa 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 (Dz. U. z 2017r., poz. 2247)[2].
1.1 Dokumenty z zakresu bezpieczeństwa informacji. Zaangażowanie kierownictwa podmiotu.	
Podstawa prawna	**§ 20 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.* **§ 20 ust. 2 pkt 1 rozporządzenia KRI:** *Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez: zapewnienie aktualizacji regulacji wewnętrznych w zakresie dotyczącym zmieniającego się otoczenia.* **§ 20 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 § 20 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 Wojewódzkim Inspektoracie Nadzoru Budowlanego w Szczecinie[3] w okresie objętym kontrolą (w zakresie bezpieczeństwa informacji) obowiązywało *Zarządzenie nr 6/2018 Zachodniopomorskiego Wojewódzkiego Inspektora Nadzoru Budowlanego z dnia 6 czerwca 2018 r. w sprawie ustalenia Polityki Bezpieczeństwa Informacji w Wojewódzkim Inspektoracie Nadzoru Budowlanego w Szczecinie*. W wyniku analizy dokumentacji związanej z bezpieczeństwem informacji stwierdzono, że funkcjonujące w Jednostce procedury spełniają wymogi określone w § 20 ust. 2 pkt 1 rozporządzenia KRI w zakresie bezpieczeństwa informacji. Procedura zawiera między innymi	

[1] Inspektor Ochrony Danych - dalej IOD.
[2] Zwane dalej rozporządzeniem KRI
[3] Zwanym dalej WINB/ Inspektoratem

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. Dyrektywa § 20 ust. 2 pkt 1 rozporządzenia KRI wskazuje na konieczność *zapewnienia aktualizacji regulacji wewnętrznych w zakresie dotyczącym zmieniającego się otoczenia*. Stwierdzono, że obowiązująca w Jednostce dokumentacja była poddana przeglądowi i weryfikacji pod kątem jej aktualizacji.
Mając na względzie powyższe, należy stwierdzić, że w WINB 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. 46, 53-127)

1.2. Analiza zagrożeń związanych z przetwarzaniem informacji

Podstawa prawna	**§ 20 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
W WINB zostały opracowane oraz zatwierdzone regulacje wewnętrzne opisujące sposób zarządzania ryzykiem w bezpieczeństwie informacji, w postaci procedury *Analiza ryzyka* stanowiącej załącznik nr 5 do Polityki Bezpieczeństwa Informacji.
Kontrolującym przedstawiono następujące dokumenty potwierdzające przeprowadzanie okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji, dotyczące okresu objętego kontrolą:

- Analizę ryzyka, sporządzoną w 2018 r.
- Analizę ryzyka infrastruktury informatycznej WINB. Aktualizacja wrzesień 2022.

Zgodnie z wyjaśnieniami Zachodniopomorskiego Wojewódzkiego Inspektora Nadzoru Budowlanego z 24 marca 2023 r. dokumentacja dotycząca analizy ryzyka została zmodyfikowana po wprowadzeniu przez Prezesa Rady Ministrów trzeciego stopnia alarmowego CRP (CHARLIE-CRP) oraz drugiego stopnia alarmowego BRAVO, natomiast w latach 2020-2021 ze względu na brak czynników, które warunkowałyby konieczność przeprowadzenia zmian analiza ryzyka nie była poddawana korekcie.
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. Działania Inspektoratu w tym zakresie realizują dyspozycję, o której mowa w § 20 ust. 2 pkt 3 rozporządzenia KRI.

(dowód: akta kontroli str. 46, 112-151)

1.3. Inwentaryzacja sprzętu i oprogramowania informatycznego

Podstawa prawna	**§ 20 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 § 20 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, zgodnie z pkt 8.1.1 normy PN-ISO/IEC 27002:2014, wszystkie aktywa informatyczne powinny być zidentyfikowane oraz powinien być sporządzany i aktualizowany ich spis. Inwentaryzacja m.in. sprzętu informatycznego powinna także zawierać informację o jego rodzaju i konfiguracji, przez co możliwe będzie jego odtworzenie po katastrofie lub innym zdarzeniu losowym.
W trakcie kontroli kontrolującym przedstawiono rejestr komputerów, urządzeń i oprogramowania służącego do przetwarzania informacji. Ustalono, że w ewidencji ujęto wszystkie urządzenia oraz oprogramowanie funkcjonujące w WINB. Mając na uwadze powyższe stwierdzono, że w Inspektoracie jest prowadzona inwentaryzacja sprzętu i oprogramowania, zgodnie z wymogami rozporządzenia KRI.

(dowód: akta kontroli str. 254)

1.4. Zarządzanie uprawnieniami do pracy w systemach informatycznych

Podstawa prawna	**§ 20 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.* **§ 20 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 § 20 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 Informacji* w postaci *Procedury nadawania uprawnień do przetwarzania danych osobowych w systemie/zbiorze danych.* Zgodnie z regulacjami przyjętymi w Inspektoracie uprawnienia w zakresie dostępu do systemu informatycznego nadaje Administrator Systemów Informatycznych lub Lokalny Administrator Systemów Informatycznych na podstawie pisemnego wniosku Właściciela Systemu Informatycznego, dzięki czemu proces nadawania i odbierania oraz modyfikacji uprawnień jest w pełni potwierdzony.
Kontrolującym przedstawiono:

- *upoważnienia do dostępu do danych osobowych w Wojewódzkim Inspektoracie Nadzoru Budowlanego* wystawione pracownikom Jednostki. W upoważnieniu wskazano system informatyczny, w którym będą przetwarzane dane osobowe oraz okres jego ważności,
- *oświadczenia o zachowaniu tajemnicy danych osobowych,* w których zawarto między innymi oświadczenie pracownika o zachowaniu w tajemnicy przetwarzanych danych, wskazując okres obowiązywania zobowiązania również na okres po ustaniu stosunku pracy,

- *wnioski dotyczące uprawnień użytkownika systemu informatycznego,*
- *wnioski dotyczące uprawnień użytkownika systemu EZD,*
- *oświadczenia o zapoznaniu się z Polityką Bezpieczeństwa Informacji Wojewódzkiego Inspektoratu Nadzoru Budowlanego w Szczecinie.*

W trakcie kontroli dokonano sprawdzenia odbierania uprawnień dostępu do systemów informatycznych pracownikom, z którymi rozwiązano stosunek pracy. Stwierdzono nieprawidłowości polegające na niezachowaniu wymogu bezzwłocznego odebrania uprawnień w systemach informatycznych. W przypadku pracownika E.S. konto zablokowano po 5 miesiącach a w przypadku pracownika D.W. konto zablokowano po 6 miesiącach od momentu rozwiązania stosunku pracy.

(dowód: akta kontroli str. 174, 185-194)

1.5. Szkolenia pracowników zaangażowanych w proces przetwarzania informacji

Podstawa prawna	**§ 20 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

W okresie objętym kontrolą (27 lutego 2023 r.) w WINB przeprowadzono szkolenie pracowników z zakresu bezpieczeństwa teleinformatycznego i ochrony danych osobowych. Udział w szkoleniu dokumentowała lista obecności zawierająca imię i nazwisko uczestnika; nazwę komórki organizacyjnej, w której zatrudniony jest pracownik oraz własnoręczny podpis. Ponadto pracownicy Inspektoratu, zostali zobligowani do zapoznania się (w formie samodzielnej pracy) z informacjami dotyczącymi bezpieczeństwa teleinformatycznego, przekazanymi im drogą elektroniczną. Z przedstawionej dokumentacji oraz złożonych przez IOD wyjaśnień wynika, że zakres tematyczny szkoleń przeprowadzonych w WINB obejmował zagadnienia wskazane w § 20 ust. 2 pkt 6 rozporządzenia KRI.

Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienie szkolenia osób zaangażowanych w proces przetwarzania informacji. Kontrolujący sugerują, aby szkolenia, których celem jest zagwarantowanie bezpieczeństwa w zakresie przetwarzania informacji miały charakter cykliczny. Ze względu na zmieniające się zagrożenia związane z dynamicznym rozwojem technologii informatycznych winny one obejmować zagadnienia wskazane w § 20 ust. 2 pkt 6 rozporządzenia KRI.

(dowód: akta kontroli str. 175-180)

1.6. Procedury zgłaszania incydentów naruszenia bezpieczeństwa informacji

Podstawa prawna	**§ 20 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

W rozdziale 7 PBI *Zgłaszanie incydentów naruszenia bezpieczeństwa informacji* określono

sposób postępowania w przypadku stwierdzenia naruszenia danych osobowych, wskazując jednocześnie katalog zdarzeń, które mogą wskazywać na wystąpienie incydentu naruszenia tych danych. Procedura przedstawia ponadto zadania przypisane administratorowi danych w przypadku powzięcia informacji o naruszeniu danych osobowych. W *Procedurze zgłaszania incydentu dotyczącego bezpieczeństwa informatycznego związanego z ochroną cyberprzestrzeni* będącej elementem *Polityki Bezpieczeństwa Informacji w Wojewódzkim Inspektoracie Nadzoru Budowlanego w Szczecinie* określono sposób zgłaszania incydentów związanych z brakiem poprawnego funkcjonowania środków zabezpieczających lub procedur bezpieczeństwa związanych z przetwarzaniem informacji. Zgodnie z § 20 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 Inspektoracie w tym zakresie wypełnia dyspozycję przywołanego powyżej rozporządzenia KRI.

Kontrolującym przedstawiono *Rejestry incydentów bezpieczeństwa i działań korygujących i zapobiegawczych* z lat objętych kontrolą, które nie zawierają wpisów ze względu na fakt, że w WINB nie odnotowano incydentów naruszenia bezpieczeństwa informacji. (dowód: akta kontroli str. 66-70, 76, 86, 182-184)

1.7. Audyt wewnętrzny z zakresu bezpieczeństwa informacji

Podstawa prawna	**§ 20 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 myśl § 20 ust. 2 pkt 14 rozporządzenia KRI, zarządzanie bezpieczeństwem informacji realizowane jest m.in. poprzez zapewnienie przez kierownictwo podmiotu publicznego warunków umożliwiających realizację i egzekwowanie działania polegającego na okresowym audycie wewnętrznym w zakresie bezpieczeństwa informacji, nie rzadziej niż raz na rok. Audyt wewnętrzny stanowi istotne źródło informacji dla kierownictwa Jednostki o realnym stanie bezpieczeństwa, różnych aspektach jego utrzymania oraz wskazuje obszary wymagające podjęcia działań korygujących.

Kontrolującym przedstawiono następujące dokumenty dotyczące okresu objętego weryfikacją:

- *Wystąpienie pokontrolne ze stanu bezpieczeństwa teleinformatycznego i ochrony danych osobowych w zakresie zgodności infrastruktury informatycznej WINB z Rozporządzeniem KRI*. Data protokołu 23 czerwca 2021 r.
- *Wystąpienie pokontrolne ze stanu bezpieczeństwa teleinformatycznego i ochrony danych osobowych w zakresie zgodności infrastruktury informatycznej WINB z Rozporządzeniem KRI*. Data protokołu 18 listopada 2022 r.

W 2020 roku w WINB nie został przeprowadzony audyt wewnętrzny z zakresu bezpieczeństwa informacji. Zgodnie z wyjaśnieniami Zachodniopomorskiego Wojewódzkiego Inspektora Nadzoru Budowlanego z 24 marca 2023 r. *odstąpiono od audytu z powodu obowiązywania w Polsce stanu epidemii, który został wprowadzony rozporządzeniem Ministra Zdrowia od 20 marca 2020 r. w związku z wprowadzonymi ograniczeniami w urzędach.*

Audyty wewnętrzne realizowane w latach 2020-2022 obejmowały swym zakresem zagadnienia związane z bezpieczeństwem informacji, wobec czego w tym okresie spełniono wymogi określone w § 20 ust. 2 pkt 14 rozporządzenia KRI.

(dowód: akta kontroli str. 46, 152-173)	
1.8. Kopie zapasowe	
Podstawa prawna	**§ 20 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 § 20 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 tworzenia kopii zapasowych zbiorów danych oraz programów uregulowane zostały w *Polityce Bezpieczeństwa Informacji w Wojewódzkim Inspektoracie Nadzoru Budowlanego w Szczecinie.* Zgodnie z wyjaśnieniami Zachodniopomorskiego Wojewódzkiego Inspektora Nadzoru Budowlanego z 27 marca 2023 r. oraz wyjaśnień Administratora systemu codziennie wykonuje się kopie zapasowe systemu EZD oraz innych systemów działających w WINB . Z powyższych wyjaśnień wynika również, że realizowane jest próbne testowane w celu sprawdzenia poprawności wykonania kopii bezpieczeństwa, przy czym nie sporządza się dokumentacji potwierdzającej przeprowadzenie testów ze uwagi na fakt, że system do wykonywania kopii bezpieczeństwa weryfikuje poprawność tego procesu i odnotowuje fakt weryfikacji stworzonych kopii. Kontrolujący przyjmują powyższe wyjaśnienia. (dowód: akta kontroli str. 22, 74)	
1.9. Wdrożone i wykorzystywane rozwiązania organizacyjne i techniczne zapewniające bezpieczeństwo informacji	
Podstawa prawna	**§ 20 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.*
Ustalenia kontroli W celu ustanowienia zabezpieczeń uniemożliwiających osobom nieuprawnionym modyfikację, usunięcie lub zniszczenie informacji każdemu pracownikowi WINB 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 9 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.
W wyniku przeglądu obowiązującej dokumentacji stwierdzono, że w rozdziale 15 PBI, w pkt 15.3-15.4 *Procedury bezpiecznej eksploatacji systemów* zostały określone zasady bezpiecznego korzystania z zasobów informatycznych, użytkowania sieci komputerowej oraz korzystania z internetu i poczty elektronicznej,

(dowód: akta kontroli str. 81-84, 181)

1.10. Rozliczalność działań w systemach teleinformatycznych.

Podstawa prawna	**§ 21 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.* **§ 21 ust. 3 rozporządzenia KRI:** *w zakresie wynikającym z analizy ryzyka poza informacjami wymienionymi w § 21 ust. 2 rozporządzenia KRI są 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.* **§ 21 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 Administratora systemu logi systemów finansowo-księgowych oraz

kadrowych: FK, KADRY-PŁACE gromadzone są w bazie danych SQL. Istotne jest ustalenie przyczyny braku możliwości przeglądania logów bezpośrednio w ww. programach, szczególnie pod kątem niezaimplementowania przez producenta oprogramowania funkcji związanej z zapisem w logach systemu faktów nadawania i odbierania uprawnień użytkownikom. Zapewnienie rozliczalności operacji polega bowiem na gromadzeniu informacji o tym, kto, kiedy i jakie działania wykonał w systemie teleinformatycznym, szczególnie gdy przetwarzanie danych podlega prawnej ochronie. Brak zapisów w logach systemu narusza § 21 ust. 2 rozporządzenia KRI, stanowiącego, że *w dziennikach systemów odnotowuje się obligatoryjnie działania użytkowników (...) polegające na dostępie do (...) systemu z uprawnieniami administracyjnymi(...).*

Zgromadzone logi przechowywane są przez okres ponad 2 lat, co jest zgodne z § 21 ust. 4 rozporządzenia KRI.

Zgodnie z wyjaśnieniami Zachodniopomorskiego Wojewódzkiego Inspektora Nadzoru Budowlanego z 27 marca 2023 r. *codziennie prowadzone są działania związane z analizą logów*, w celu identyfikacji działań niepożądanych.

(dowód: akta kontroli str. 21, 50, 275-276)

Stwierdzone nieprawidłowości w obszarze nr 1:

1. Nieodnotowywanie w dziennikach systemów finansowo-księgowych oraz kadrowych: FK, KADRY-PŁACE działań użytkowników z uprawnieniami administracyjnymi, co nie wypełnia dyspozycji § 21 ust. 2 rozporządzenia KRI.
   W związku z informacją Zachodniopomorskiego Wojewódzkiego Inspektora Nadzoru Budowlanego z dnia 11 lipca 2023 r., że systemy finansowo-księgowe oraz kadrowo-płacowe zostały zaktualizowane na spełniające stawiane im wymagania dotyczące rozliczalności - odstępuje się od sformułowania zaleceń w tym zakresie.
2. Niezachowanie wymogu bezzwłocznego odebrania uprawnień w systemach informatycznych pracownikowi, z którym rozwiązano stosunek pracy, zgodnie z dyspozycją § 20 ust. 2 pkt 5 rozporządzenia KRI.

Ocena obszaru kontroli	**Pozytywna z nieprawidłowościami**

Obszar 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], zwane dalej „*rozporządzeniem RODO*”

2.1 Wyznaczenie IOD

Ustalenia kontroli

Formalne wyznaczenie IOD w Wojewódzkim Inspektoracie Nadzoru Budowlanego w oparciu o zapisy ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych nastąpiło 17 lipca 2018 r., Zarządzeniem nr 12/2018 Zachodniopomorskiego Wojewódzkiego Inspektora Nadzoru Budowlanego w sprawie powołania Inspektor Ochrony Danych. Zgodnie z wymogiem określonym w art. 37 ust. 7 RODO oraz art. 11 Ustawy o ochronie danych osobowych dane Inspektora Ochrony Danych, sposób i formę kontaktu opublikowano w Biuletynie Informacji Publicznej WINB. Stwierdzono, że na dzień badania powyższe dane były aktualne a osoba

[4] Dz. Urz. UE L2016.119.

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. 236-248)

2.2 Rejestr czynności przetwarzania

Ustalenia kontroli

Zgodnie z *Zarządzeniem nr 12/2018 Zachodniopomorskiego Wojewódzkiego Inspektora Nadzoru Budowlanego w sprawie powołania Inspektor Ochrony Danych* prowadzenie rejestru czynności przetwarzania w kontrolowanej Jednostce powierzono IOD. W WINB 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 2023 r. rejestr czynności przetwarzania liczył 29 pozycji (celów przetwarzania).

(dowód: akta kontroli str. 260-261)

2.3 Rejestr kategorii czynności przetwarzania

Ustalenia kontroli

Zgodnie z oświadczeniem Zachodniopomorskiego Wojewódzkiego Inspektora Nadzoru Budowlanego z dnia 24 marca 2023 r. w WINB nie są realizowane czynności związane z przetwarzaniem danych osobowych na rzecz innego administratora. W związku z powyższym nie jest prowadzony Rejestr kategorii czynności przetwarzania.

(dowód: akta kontroli str. 46)

2.4 Rejestr incydentów

Ustalenia kontroli

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 wobec tego wymogu 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[5] wskazuje, 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.

W WINB utworzono rejestr incydentów. Rejestr prowadzony jest w formie elektronicznej. Na dzień przeprowadzenia kontroli IOD wyjaśnił, że w WINB w badanym okresie nie było naruszeń. Rejestr zawiera następujące pozycje: l.p. incydentu, osoba zgłaszająca, 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.

[5] 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.

2.5 Analiza ryzyka

Ustalenia kontroli

W WINB, w badanym okresie przeprowadzono analizę ryzyka w zakresie ochrony danych osobowych. Przedstawiony kontrolującym dokument *Analiza ryzyka w zakresie ochrony danych osobowych w Wojewódzkim Inspektoracie Nadzoru Budowlanego w Szczecinie* opisuje metodykę szacowania ryzyka. Załącznikiem do wyżej opisanej procedury jest macierz z przypisanymi wartościami.

(dowód: akta kontroli str. 221-235)

2.6 Klauzula informacyjna

Ustalenia kontroli

Na stronie internetowej WINB 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 Inspektor Ochrony Danych.

Klauzula informacyjna została również wywieszona na tablicy w siedzibie WINB. Przygotowano również klauzulę informacyjną dla pracowników.

(dowód: akta kontroli str. 248-253)

2.7 Szkolenia

Ustalenia kontroli

W okresie objętym kontrolą (27 lutego 2023 r.) w WINB przeprowadzono szkolenie pracowników z zakresu ochrony danych osobowych. Udział w szkoleniu dokumentowała lista obecności zawierająca imię i nazwisko uczestnika, własnoręczny podpis oraz wskazanie komórki organizacyjnej, w której zatrudniono pracownika.

(dowód: akta kontroli str. 177-180)

2.8 Umowy powierzenia przetwarzania danych osobowych

Ustalenia kontroli

Zgodnie z art. 28 ust. 3 i ust. 9 rozporządzenia RODO, w badanym okresie WINB zawarł następujące umowy powierzenia przetwarzania danych osobowych:

- Umowa powierzenia przetwarzania danych osobowych poczty elektronicznej zawarta 28 lutego 2023 r. XXX,
- Umowa powierzenia przetwarzania danych osobowych XXX zawarta dnia 11 grudnia 2020 r. XXX,
- Umowa powierzenia przetwarzania danych osobowych XXX zawarta 26 września 2018 r. 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 pozyskanych informacji.

W WINB, zgodnie z oświadczeniem Zachodniopomorskiego Wojewódzkiego Inspektora Nadzoru Budowlanego z dnia 27 marca 2023 r. dokonano weryfikacji podmiotów przetwarzających, pod kątem zapewnienia wystarczających gwarancji wdrożenia odpowiednich

środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r.[6] i chroniło prawa osób, których dane dotyczą. (dowód: akta kontroli str. 24-45, 195-212)	
Stwierdzone nieprawidłowości w obszarze nr 2 : nie stwierdzono nieprawidłowości	
Ocena obszaru kontroli nr 2	**Pozytywna**
Wnioski dotyczące uzyskanych efektów zrealizowanego zadania	Istotną kwestią z punktu widzenia bezpieczeństwa informacji jest ciągłe podnoszenie świadomości pracowników (poprzez realizację różnych form szkoleń) w zakresie istnienia potencjalnych zagrożeń oraz wiedza w jaki sposób postępować w przypadku materializacji ryzyk związanych z naruszeniem bezpieczeństwa wszystkich przetwarzanych przez Jednostkę informacji (ze szczególnym uwzględnieniem naruszenia ochrony danych osobowych). Należy na bieżąco podejmować działania mające na celu zabezpieczenie danych, między innymi poprzez bezzwłoczne blokowanie dostępu do systemów informatycznych osobom pozbawionym uprawnień.
Zalecenie	Bezzwłocznie odbierać uprawnienia w systemach informatycznych pracownikom, z którymi rozwiązano stosunek pracy, do czego zobowiązuje zapis § 20 ust. 2 pkt 5 rozporządzenia KRI.
Pouczenie	– od wystąpienia pokontrolnego nie przysługują środki odwoławcze; – o podjętych działaniach, mających na celu wyeliminowanie stwierdzonych nieprawidłowości, 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 Mateusz Wagemann II Wicewojewoda Zachodniopomorski

[6] Rozporządzenie Parlamentu Europejskiego i Rady UE 2016/679 z dn. 27.04.20165 r. w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE7.04.2016 r. w sprawie ochrony osób fizycznych.