WOJEWODA
ZACHODNIOPOMORSKI

WPŁYNĘŁO
Kuratorium Oświaty w Szczecinie
KANCELARIA
22. 05. 2020
Ilość załączników.....
Podpis.....

P. dyr M. Świecka
22.05.2020 r.

Szczecin, dnia 21 maja 2020 r.

Znak: K-2.1611.2.2019.IO

Pani
Magdalena Zarębska-Kulesza
Zachodniopomorski Kurator Oświaty

Szanowna Pani Kurator,

W związku z odstąpieniem od wniesienia pisemnych, umotywowanych zastrzeżeń do ustaleń zawartych w projekcie wystąpienia pokontrolnego przekazanego pismem z dnia 24 kwietnia 2020r., w załączeniu przedkładam wystąpienie pokontrolne z kontroli planowej przeprowadzonej w dniach 17-30 września 2019 r w Kuratorium Oświaty w Szczecinie w zakresie bezpieczeństwa systemów teleinformatycznych wykorzystywanych do realizacji zadań publicznych oraz ochrony danych osobowych, w tym stanu wdrożenia RODO.

O podjętych działaniach, mających na celu wyeliminowanie stwierdzonych nieprawidłowości, proszę poinformować mnie za pośrednictwem Wydziału Kontroli Zachodniopomorskiego Urzędu Wojewódzkiego w Szczecinie, w terminie 2 miesięcy od daty otrzymania niniejszego wystąpienia.

Z poważaniem,
WZ. WOJEWODY ZACHODNIOPOMORSKIEGO
Marek Subocz
WICEWOJEWODA

Zachodniopomorski Urząd Wojewódzki w Szczecinie
Wydział Kontroli
Wały Chrobrego 4, 70-502 Szczecin
tel. 91 43 03 554
www.szczecin.uw.gov.pl, e-mail: wk@szczecin.uw.gov.pl

WOJEWODA
ZACHODNIOPOMORSKI

Szczecin, dnia 21 maja 2020 r.

Znak: K-2.1611.2.2019.IO

WYSTĄPIENIE POKONTROLNE

Przedmiot kontroli	1. **Bezpieczeństwo systemów teleinformatycznych wykorzystywanych do realizacji zadań publicznych.** 2. **Ochrona danych osobowych, stan wdrożenia RODO.**
Nazwa i adres organu kontrolującego	Wojewoda Zachodniopomorski, ul. Wały Chrobrego 4, 70-502 Szczecin
Nazwa i adres organu kontrolowanego	Zachodniopomorski Kurator Oświaty[1], 70-502 Szczecin, Wały Chrobrego 4
Osoba pełniąca funkcję ZKO w okresie objętym kontrolą oraz w okresie prowadzenia kontroli	Pani Magdalena Zarębska-Kulesza
Okres objęty kontrolą	Od dnia 1 stycznia 2017 r. do dnia 30 września 2019 r.
Kontrolujący	Pracownicy Zachodniopomorskiego Urzędu Wojewódzkiego w Szczecinie (ZUW): - Jan Kępiński - informatyk wojewódzki w Biurze Organizacji i Kadr, Inspektor Ochrony Danych ZUW, *kierownik zespołu kontrolnego*, - Iwona Olesińska – inspektor wojewódzki.
Nr upoważnienia	Nr 105/19 z dnia 2.09.19 r. oraz nr 105/2/19 z dnia 20.09.19 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 2011r. o kontroli w administracji rządowej (Dz. U. z 2020 r., poz. 224), - art. 28 ust. 1 pkt 1 ustawy z dnia 23 stycznia 2009r. o wojewodzie i administracji rządowej w województwie (Dz.U. z 2019 r., poz. 1464).
Kryteria prowadzenia kontroli	legalność, rzetelność
Termin kontroli	17 września – 30 września 2019 r.
Osoby udzielające wyjaśnień w trakcie kontroli	1. Pani Monika Świercz -Dyrektor Wydziału Administracji i Kadr. 2. Pan Michał Kazimierczuk- Starszy informatyk, Inspektor Ochrony Danych[2]. 3. Pan Łukasz Słodkowski – Główny specjalista administrator sieci[3].

[1] Zwany dalej ZKO lub Kuratorem.
[2] Zwany dalej IOD.
[3] Zwany dalej informatykiem Urzędu.

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)[4].
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

W Kuratorium Oświaty w Szczecinie[5] w okresie objętym kontrolą obowiązywały następujące uregulowania w zakresie bezpieczeństwa informacji:

- Zarządzenie Nr 46/2015 Zachodniopomorskiego Kuratora Oświaty z dnia 5 października 2015 r. w sprawie ustalenia Polityki Bezpieczeństwa Informacji oraz instrukcji zarządzania systemem informatycznym w Kuratorium Oświaty w Szczecinie,
- Zarządzenie Nr 27/2018 Zachodniopomorskiego Kuratora Oświaty z dnia 8 czerwca 2018 r. w sprawie ustalenia Polityki Bezpieczeństwa w Kuratorium Oświaty w Szczecinie,
- Zarządzenie Nr 43/2019 Zachodniopomorskiego Kuratora Oświaty z dnia 2 sierpnia 2019 r. w sprawie ustalenia Polityki Bezpieczeństwa oraz instrukcji zarządzania systemem informatycznym w Kuratorium Oświaty w Szczecinie.

W wyniku analizy obowiązującej dokumentacji stwierdzono, że w Kuratorium nie zostały opracowane kompletne regulacje wewnętrzne składające się na system zarządzania bezpieczeństwem informacji[6], w szczególności nie opracowano kompletnej polityki bezpieczeństwa informacji, co jest niezgodne z § 20 ust. 1 rozporządzenia KRI stanowiącego, że 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,

[4] Zwane dalej rozporządzeniem KRI.
[5] Zwane dalej Kuratorium.
[6] Zwany dalej SZBI.

jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność. Ponadto § 20 ust. 3 rozporządzenia KRI wskazuje, że wymagania określone w ww. ust. 1 uznaje się za spełnione, jeżeli system zarządzania bezpieczeństwem informacji został opracowany na podstawie Polskiej Normy PN-EN ISO/IEC 27001, a ustanawianie zabezpieczeń, zarządzanie ryzykiem oraz audytowanie odbywa się na podstawie Polskich Norm związanych z tą normą. W pkt. 5.1 normy PN-EN ISO/IEC 27002 wskazano opracowanie i stosowanie dokumentu polityki bezpieczeństwa informacji. Stwierdzono ponadto, że nie opracowano zasad i procedur postępowania w kluczowych elementach dotyczących projektowania, wdrażania, monitorowania czy rozliczalności systemów teleinformatycznych. Ustalono natomiast, że w związku z wejściem w życie przepisów RODO[7], w Kuratorium Oświaty w Szczecinie dokonano aktualizacji Polityki bezpieczeństwa oraz Instrukcji zarządzania systemem informatycznym, pod kątem dostosowania do wymogów tego rozporządzenia.

(dowód: akta kontroli str. 151-269)

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 celu określenia potrzeb organizacji w odniesieniu do wymagań związanych z bezpieczeństwem informacji oraz utworzenia skutecznego SZBI niezbędne jest systematyczne podejście do zarządzania ryzykiem. Zaleca się, aby zarządzanie ryzykiem w bezpieczeństwie informacji było integralną częścią wszystkich działań związanych z tym obszarem oraz zostało zastosowane zarówno do wdrożenia, jak i w ciągłej eksploatacji SZBI. Przystępując do procesu szacowania ryzyka należy określić zakres procesu zarządzania ryzykiem, tak aby zapewnić, że analiza ryzyka uwzględni wszystkie aktywa. Zgodnie z normą PN-ISO/IEC 27000 aktywem jest wszystko, co ma wartość dla organizacji np.: oprogramowanie, takie jak program komputerowy; fizyczne, takie jak komputer; usługi; personel i jego kwalifikacje, umiejętności i doświadczenie; wartości niematerialne, takie jak reputacja i wizerunek.

Minimalnym wymogiem spełniającym warunek przeprowadzenia okresowej analizy ryzyka powinna być jej realizacja przed wykonaniem corocznego audytu bezpieczeństwa informacji. Pozwoli to bowiem na objęcie audytem w szczególności tych zagadnień, w których ujawniono najwyższe ryzyka wystąpienia zagrożeń.

W trakcie kontroli kontrolującym przedstawiono *Rejestr ryzyka Kuratorium Oświaty w Szczecinie systemu teleinformatycznego na dzień 31.12.2016 r.* oraz *Rejestr ryzyka Kuratorium Oświaty w Szczecinie Ochrony Danych Osobowych*, będący załącznikiem nr 2 do *Polityki Bezpieczeństwa Informacji Kuratorium Oświaty w Szczecinie,* obowiązującej w Jednostce od 8 czerwca 2018 r.

W zakresie zarządzania ryzykiem stwierdzono nieprawidłowości polegające na przeprowadzeniu analizy ryzyka w niepełnym zakresie, szczególnie w przypadku analizy ograniczonej do ryzyka odnoszącego się do ochrony danych osobowych.

Finalnym dokumentem procesu zarządzania ryzykiem winien być plan postępowania z ryzykiem, na który składa się określenie aktywów, wyszczególnienie ryzyk i zagrożeń, identyfikacja

[7] 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)[7], zwane dalej RODO.

podatności i następstw, wskazanie zabezpieczeń oraz ocena ryzyka. Kontrolującym nie przedstawiono planu postępowania z ryzykiem.

(dowód: akta kontroli str. 33-37, 253-255)

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. Aktualna 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 przedstawiono kontrolującym aktualny rejestr komputerów, urządzeń i oprogramowania służącego do przetwarzania informacji, o którym mowa w § 20 ust. 2 pkt 2 rozporządzenia KRI.

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.

W Kuratorium wprowadzono zasady w zakresie dokumentowania nadawania, zmiany i odbierania uprawnień dla użytkowników systemów teleinformatycznych, które wspierają zapewnianie przejrzystości i rozliczalności działań użytkowników w systemach. Nadanie, zmiana, odebranie uprawnień następuje na wniosek przesłany pocztą elektroniczną do administratora systemu.

(dowód: akta kontroli str. 70-73, 82-92, 110, 247)

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

§ 20 ust. 2 pkt 6 rozporządzenia KRI stanowi, że podmiot realizujący zadania publiczne zapewnienia szkolenie osób zaangażowanych w proces przetwarzania informacji.
W kontrolowanym okresie w Kuratorium przeprowadzono 2 szkolenia obejmujące swym zakresem zagadnienia bezpieczeństwa teleinformatycznego, w tym:
- zagrożenia bezpieczeństwa informacji,
- skutki naruszenia zasad bezpieczeństwa informacji, w tym odpowiedzialność prawna,
- stosowanie środków zapewniających bezpieczeństwo informacji, w tym urządzenia i oprogramowanie minimalizujące ryzyko błędów ludzkich.

Ponadto przeprowadzono szkolenie z zakresu ochrony danych osobowych i RODO.

(dowód: akta kontroli str. 104, 106)

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 wyniku analizy przedstawionej dokumentacji dotyczącej postępowania w przypadku naruszenia bezpieczeństwa informacji ustalono, że w Jednostce określono sposób umożliwiający szybkie podjęcie działań korygujących oraz określono zasady dokumentowania skutków stwierdzonego naruszenia ochrony danych osobowych, wymagane art. 33 ust. 5 rozporządzenia RODO. Procedura zgłaszania incydentów powinna jednak obejmować zdarzenia i zagrożenia nie tylko w kontekście ochrony danych osobowych, ale winna dotyczyć naruszenia bezpieczeństwa wszystkich informacji przetwarzanych w Jednostce.
Niezależnie od działań pracowników incydenty winny być sygnalizowane przez alerty z systemów zabezpieczeń (firewall, IPS, antywirus itp.), komunikaty z systemu zarządzania zdarzeniami, raporty o nieprawidłowościach weryfikacji integralności plików czy logi z systemów operacyjnych.
Brak procedur i niedokonywanie weryfikacji zapisów w dziennikach zdarzeń (wynikające m.in. z braku odpowiedniej funkcjonalności systemów pod kątem wykrywania incydentów bezpieczeństwa informacji w obszarze systemów IT) uniemożliwiało i uniemożliwi w przyszłości ograniczanie wpływu przypadków naruszeń bezpieczeństwa aktywów informacyjnych na ciągłość operacyjną procesów, systemów i infrastruktury teleinformatycznej kontrolowanej Jednostki.

(dowód: akta kontroli str. 263-264)

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.
W badanym okresie w Kuratorium nie przeprowadzono kompleksowego audytu wewnętrznego w zakresie bezpieczeństwa informacji, czym nie wypełniono dyspozycji § 20 ust. 2 pkt 14 rozporządzenia KRI. W rezultacie kierownik kontrolowanej Jednostki może nie dysponować rzetelną oceną skuteczności przyjętych rozwiązań w zakresie bezpieczeństwa informacji.

(dowód: akta kontroli str. 111)

8. *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 pkt 6.2 *Polityki bezpieczeństwa* oraz w pkt 1.2 *Instrukcji zarządzania systemem informatycznym* zostały określone obowiązki, odpowiedzialność, zasady i ograniczenia, dotyczące instalacji przez pracowników oprogramowania na jednostkach komputerowych. Na podstawie oględzin użytkowanych komputerów ustalono, że we wszystkich przypadkach użytkownicy nie mieli przyznanych uprawnień administracyjnych umożliwiających instalację dowolnego oprogramowania.
Instrukcja zarządzania systemem informatycznym określa zasady nadawania, aktualizacji i wycofania uprawnień do przetwarzania danych osobowych w systemach informatycznych. Określa również zasady rejestrowania tych uprawnień oraz metody i środki uwierzytelnienia użytkowników w systemach informatycznych. Na podstawie badania próby 10 użytkowników systemów informatycznych ustalono, że wszyscy posiadali uprawnienia do pracy w systemach adekwatne do zakresu realizowanych zadań.

Sprawdzeniu podlegało blokowanie uprawnień użytkowników po ustaniu zatrudnienia. Zgodnie z oświadczeniem informatyka Urzędu blokowanie kont dostępu do systemów informatycznych pracowników rozwiązujących stosunek pracy następuje po otrzymaniu telefonicznej lub osobiście przekazanej informacji z Wydziału Administracji i Kadr. Nierealizowanie wymogu dokumentowania powyższych czynności, w postaci pisemnego wniosku osób upoważnionych, powoduje, że proces nadawania i odbierania uprawnień nie jest w pełni potwierdzony.
We wszystkich systemach działających w Kuratorium zmiana haseł dostępu była wymuszana automatycznie (komputery są zarządzane centralnie w oparciu o mechanizm Microsoft Active Directory). Wymogi dotyczące złożoności haseł do systemów informatycznych zostały określone w pkt 1.1 *Instrukcji zarządzania systemem informatycznym* oraz w pkt 6.2 *Polityki bezpieczeństwa*. Zdefiniowano m.in.: maksymalny okres ważności hasła - 30 dni, minimalną długość hasła - 8 znaków, wymagania co do złożoności hasła. Powyższe rozwiązania i wymogi określone w instrukcji były zgodne z § 20 ust. 2 pkt 7 rozporządzenia KRI.
W trakcie oględzin stwierdzono, że na wszystkich stanowiskach pracy w pomieszczeniach Kuratorium ustawienie monitorów uniemożliwiało odczytanie wyświetlanych danych przez osoby nieuprawnione. Powyższe działanie spełniało wymogi § 20 ust 2 pkt 7 rozporządzenia KRI.
W wyniku przeglądu obowiązującej dokumentacji stwierdzono, że:
- w pkt 6.1 *Polityki bezpieczeństwa* określono zasadę niszczenia urządzeń oraz innych elektronicznych nośników informacji w przypadku ich likwidacji,
- w rozdziale VII oraz VIII *Instrukcji zarządzania systemem informatycznym* określone zostały procedury wykonywania napraw, przeglądów i konserwacji systemu informatycznego oraz elektronicznych nośników informacji służących do przetwarzania danych,
- zasady dotyczące tworzenia i przechowywania kopii zapasowych danych w Kuratorium zostały określone w rozdziale IV oraz VI *Instrukcji zarządzania systemem informatycznym*. Wskazano osobę odpowiedzialną za wykonywanie kopii bezpieczeństwa. Kopie bezpieczeństwa były przechowywane poza miejscem ich wytwarzania, tj. w Delegaturze Kuratorium w Koszalinie,
- w rozdziale VIII *Instrukcji zarządzania systemem informatycznym* zostały uregulowane zasady związane z zarządzaniem zmianami w wykorzystywanym oprogramowaniu,
- sporządzono pisemną procedurę testowania kopii zapasowych. Testowanie kopii, według oświadczenia informatyka Urzędu, realizowane było raz na miesiąc. W okresie objętym kontrolą nie wystąpiły przypadki konieczności odtworzenia danych z kopii zapasowych,
- w procedurach nie zostały określone zasady dotyczące postępowania w przypadku przekazywania sprzętu informatycznego poza jednostkę, np. w celu wykonania napraw,
- nie opracowano zasad (procedur) dotyczących bezpiecznej pracy przy przetwarzaniu mobilnym i pracy na odległość, o których mowa w § 20 ust. 2 pkt 8 rozporządzenia KRI. Nie została przyjęta również jednolita procedura w zakresie szyfrowania urządzeń przenośnych. Zgodnie z Oświadczeniem Pana Michała Kazimierczuka – starszego informatyka *notebooki służą głównie do prezentacji multimedialnych.*
- nie zostały określone zasady monitorowania stanu pojemności przestrzeni dyskowej w serwerach Kuratorium. Ustalono jednak, że stosownie do zalecenia sformułowanego w pkt A.12.1.3 załącznika A normy PN-ISO/IEC 27001:2017, pojemność była na bieżąco monitorowana przez informatyka.
Na podstawie oględzin 10 stanowisk komputerowych ustalono, że był na nich zainstalowany i uruchomiony program antywirusowy, który wykorzystywał aktualną na moment badania wersję bazy definicji wirusów, co było zgodne z § 20 ust. 2 pkt 12 lit. f rozporządzenia KRI. Stosownie do § 20 ust. 2 pkt 12 lit. a i f rozporządzenia KRI w Jednostce przeprowadzano aktualizacje systemów operacyjnych. Nie stwierdzono wykorzystywania systemów operacyjnych, nieobjętych wsparciem producenta (np. Windows XP).

W trakcie kontroli stwierdzono, że w Kuratorium nie opracowano planów o charakterze awaryjnym, które powinny być tworzone na wypadek sytuacji kryzysowych (określające między innymi dostęp do konkretnych miejsc czy danych w sytuacji awarii, zasady administrowania systemami informatycznymi w przypadkach nieobecności / niedostępności administratora). Brak planów awaryjnych skutkować może naruszeniem ciągłości bieżącego zarządzania dostępem do informacji i uprawnieniami użytkowników (w tym brakiem możliwości bezzwłocznego utworzenia czy blokady konta jak również odtwarzania systemów po awarii).
W celu realizacji zadań z zakresu kadrowo-płacowego kontrolowany podmiot zawarł Umowę Konserwacyjną[8] z Wojciechem Jurkowskim i Jackiem Jurkowskim, prowadzącymi działalność gospodarczą pod nazwą Datacomp S. C. Wojciech Jurkowski i Jacek Jurkowski z siedzibą w Szczecinie, obejmującą swym zakresem nadzór i konserwację systemu kadrowo-płacowego Komax 2.0. W umowie wprowadzono zapisy gwarantujące zachowanie poufności informacji przez wykonawcę umowy. Ponadto został określony maksymalny czas skutecznej naprawy oprogramowania, czym wypełniono dyspozycję § 20 ust. 2 pkt 10 rozporządzenia KRI. Z podmiotem tym zawarto również umowę powierzenia przetwarzania danych osobowych.
W trakcie oględzin pomieszczenia serwerowni stwierdzono, że Jednostka wprowadziła rozwiązania w zakresie podtrzymania zasilania oraz warunków środowiskowych pracy serwerów i urządzeń sieciowych. W pomieszczeniach użytkowanych przez Kuratorium nie zostały zainstalowane zapasowe źródła zasilania sprzętu komputerowego, tj. równoległa linia zasilająca lub agregat prądotwórczy. W okresie objętym kontrolą testowano lub serwisowano znajdujące się w serwerowni zasilacze awaryjne i klimatyzator. W pkt 6.1 *Polityki bezpieczeństwa* wskazano osoby uprawnione do dostępu do serwerowni.

(dowód: akta kontroli str. 58-65, 70-103, 105-107, 109-110, 165-268)

9. 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.*

[8] Umowa Konserwacyjna nr 2105K/2019 z dnia 1.06.2019 r.

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 co 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).
Kopie dzienników zdarzeń (logów) wg oświadczenia administratora sieci są wykonywane z całym systemem wraz z plikami i bazami kluczowych systemów i przechowywane przez okres 2 lat.
W procedurach wewnętrznych obowiązujących w Kuratorium nie uregulowano kwestii związanych z regularnym przeglądaniem logów systemów IT. W konsekwencji nie wskazano też osoby odpowiedzialnej za monitorowanie dostępu do informacji i czynności zmierzających do wykrycia nieautoryzowanych działań związanych z przetwarzaniem informacji. Istotnym czynnikiem warunkującym sprawność zarządzania incydentami bezpieczeństwa informacji jest właściwa identyfikacja incydentów, zwłaszcza w przypadkach, kiedy notyfikacje pochodzą z systemów generujących duży wolumen logów.

(dowód: akta kontroli str. 107)

Stwierdzone nieprawidłowości

- nieopracowanie kompletnych regulacji wewnętrznych składających się na system zarządzania bezpieczeństwem informacji, zgodnie z § 20 ust. 1 rozporządzenia KRI,
- brak procedur dotyczących bezpiecznej pracy przy przetwarzaniu mobilnym i pracy na odległość, wymaganych na podstawie § 20 ust. 2 pkt 8 rozporządzenia KRI,
- brak procedury regulującej kwestie szyfrowania urządzeń przenośnych, zgodne z wymogami § 20 ust. 2 pkt 9 i 11 rozporządzenia KRI,
- nieprzeprowadzanie kompleksowego audytu wewnętrznego w zakresie bezpieczeństwa informacji, o którym mowa w § 20 ust. 2 pkt 14 rozporządzenia KRI,
- przeprowadzanie analizy ryzyka w niepełnym zakresie,
- nieprzypisanie w procedurach wewnętrznych obowiązków i odpowiedzialności za przeglądanie logów systemowych,
- niedokonywanie weryfikacji zapisów w dziennikach zdarzeń,
- nieopracowanie planów o charakterze awaryjnym, na wypadek sytuacji kryzysowych.

Ocena obszaru kontroli nr 1	Zakresy szczegółowo opisane w pkt 1.1-1.6 oraz 1.8-1.9 pomimo stwierdzonych nieprawidłowości, oceniono pozytywnie. Mając natomiast na względzie wagę stwierdzonych nieprawidłowości w obszarze 1.7, polegających na nieprzeprowadzaniu corocznych audytów wewnętrznych z zakresu bezpieczeństwa informacji, do czego zobowiązują zapisy § 20 ust. 2 pkt 14 rozporządzenia KRI, wskazany zakres oceniono negatywnie.
Obszar nr 2. Ocena stanu wdrożenia RODO w Jednostce	
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)[9], zwane dalej *„rozporządzeniem RODO"*

Ustalenia kontroli

Wyznaczenie ABI, IOD

W trakcie kontroli ustalono, że:

- Zarządzeniem Nr 25/2015 Zachodniopomorskiego Kuratora Oświaty z dnia 25 maja 2015 r. na stanowisko odpowiedzialne za bezpieczeństwo informacji (Administrator Bezpieczeństwa Informacji[10]) wyznaczony został pracownik Kuratorium;
- Zarządzeniem Nr 65/2018 z 5 września 2018 Zachodniopomorski Kurator Oświaty, zgodnie z art. 37 ust. 1 lit. a RODO wyznaczył Inspektora Ochrony Danych[11];
- Zachodniopomorski Kurator Oświaty przesłał do Urzędu Ochrony Danych Osobowych zawiadomienie o wyznaczeniu IOD (wyznaczona osoba pełniła w Jednostce we wcześniejszym okresie funkcję ABI);
- Zarządzeniem Zachodniopomorskiego Kuratora Oświaty określono zakres obowiązków pracownika zatrudnionego na stanowisku IOD;
- Pracownik, któremu powierzono funkcje IOD posiadał niezbędne kompetencje do pełnienia powierzonych mu zadań poparte wykształceniem, praktyką zawodową, szkoleniami i kursami (obejmującymi również problematykę RODO);
- zgodnie z art. 11 ustawy o ochronie danych osobowych (Dz.U. z 2019 r., poz..1781 t. j.) na stronie internetowej Kuratorium udostępniono dane Inspektora Ochrony Danych;
- w kontrolowanej Jednostce spełniono wymóg art. 38 ust. 3 RODO stanowiący, że IOD podlega bezpośrednio najwyższemu kierownictwu (w przypadku Kuratorium - Zachodniopomorskiemu Kuratorowi Oświaty).[12]

(dowód: akta kontroli str.113-117)

Dokumentacja RODO

W związku z wejściem w życie przepisów RODO, w Kuratorium Oświaty w Szczecinie przeprowadzono aktualizację *Polityki bezpieczeństwa* oraz *Instrukcji zarządzania systemem informatycznym* pod kątem dostosowania do wymogów tego rozporządzenia.

Regulacje wewnętrzne w zakresie polityki bezpieczeństwa danych osobowych zostały udostępnione pracownikom Kuratorium w sieci wewnętrznej (intranet).

W trakcie kontroli stwierdzono, że wszyscy pracownicy złożyli oświadczenia o zapoznaniu się z ww. dokumentami.

(dowód: akta kontroli str. 165-269)

Rejestr czynności

Rozporządzenie RODO przewiduje, że administratorzy danych oraz podmioty przetwarzające mają obowiązek prowadzenia odpowiednio rejestru czynności.

Stosownie do art. 30 RODO, Inspektor Ochrony Danych sporządził i prowadził rejestr czynności przetwarzania. Rejestr zawierał informacje, wynikające z art. 30 RODO.

(dowód: akta kontroli str. 66-69)

---

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

[10] Zwany dalej ABI.

[11] Zwany dalej IOD.

[12] Zgodnie z rozdziałem IV, § 18a.2. Regulaminu Kuratorium Oświaty w Szczecinie stan prawny na 29 listopada 2019r. Ustalony zarządzeniem Nr 52/2013 Zachodniopomorskiego Kuratora Oświaty z dnia 21 sierpnia 2013r. w sprawie ustalenia regulaminu Kuratorium Oświaty w Szczecinie, zatwierdzonym zarządzeniem Nr 498/2013 Wojewody Zachodniopomorskiego z dnia 4 września 2013r. w sprawie zatwierdzenia regulaminu Kuratorium Oświaty w Szczecinie – tekst ujednolicony: *W ramach realizowanych zadań i obowiązków, Inspektor Ochrony Danych Osobowych podlega bezpośrednio Kuratorowi.*

Rejestr naruszeń, zgłaszanie naruszeń
W Kuratorium został utworzony rejestr naruszeń ochrony danych osobowych. W okresie objętym kontrolą w Kuratorium miało miejsce jedno naruszenie, które zostało zgłoszone do organu nadzorczego - Urzędu Ochrony Danych Osobowych.

Klauzula informacyjna
W Kuratorium w Szczecinie opracowano klauzule informacyjne dla pracowników zawierające elementy, o których mowa w art. 13 rozporządzenia RODO.

(dowód: akta kontroli str. 112)

Szkolenia
W kontrolowanym okresie (przed wejściem w życie RODO) w Kuratorium przeprowadzono szkolenia z zakresu ochrony danych osobowych i RODO.

(dowód: akta kontroli str. 108)

Umowy powierzenia
Zgodnie z art. 28 ust. 3 i ust. 9 rozporządzenia RODO, w badanym okresie Kuratorium powierzyło dane osobowe instytucjom i szkołom na mocy umów powierzenia przetwarzania danych osobowych. Zawarto również taką umowę z podmiotem realizującym zadania nadzoru i konserwacji systemu kadrowo-płacowego. Ponadto z Akademią Sztuki w Szczecinie zawarto umowę o współadministrowanie. Umowy zawierały wszystkie elementy wyszczególnione w art. 28 ww. rozporządzenia między innymi: przedmiot i czas trwania przetwarzania, charakter i cel przetwarzania, rodzaj danych osobowych, obowiązki i prawa Administratora. Zobowiązano podmioty przetwarzające do przechowywania danych zgodnie z umową i rozporządzeniem RODO oraz zachowania w tajemnicy danych osobowych i informacji dotyczących przechowywania danych.

(dowód: akta kontroli str.48-62)

Ocena obszaru kontroli nr 2	Pozytywna
Zalecenia	• Uzupełnić SZBI o zagadnienia wynikające z rozporządzenia KRI dotyczące zarządzania bezpieczeństwem informacji, zgodnie z § 20 ust. 1 rozporządzenia KRI, • Przeprowadzać corocznie audyty wewnętrzne z zakresu bezpieczeństwa informacji, zgodnie z § 20 ust. 2 pkt 14 rozporządzenia KRI. • Opracować plany o charakterze awaryjnym dotyczącym ciągłości działania Jednostki, na wypadek sytuacji kryzysowych. • Dokonywać regularnie weryfikacji zapisów w dziennikach zdarzeń. • Przypisać odpowiedzialność za przeglądanie logów systemowych w procedurach wewnętrznych. • Przeprowadzać analizy ryzyka obejmujące pełny zakres bezpieczeństwa informacji.
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 2 miesięcy od daty otrzymania niniejszego wystąpienia.
Podpis kierownika jednostki kontrolującej	wz. WOJEWODY ZACHODNIOPOMORSKIEGO *Marek Subocz* WICEWOJEWODA