Minister Funduszy
i Polityki Regionalnej

Warszawa, data: 2 kwietnia 2024 r.

znak sprawy: DKN-la.0813.5.2023.MD

**Pan**
**Łukasz Bałajewicz**
**p.o. Prezesa**
**Krajowego Zasobu Nieruchomości**

## WYSTĄPIENIE POKONTROLNE

**I. Jednostka kontrolowana:**

Krajowy Zasób Nieruchomości, ul. Nowy Świat 19, 00-029 Warszawa (dalej: KZN).

**II. Zakres kontroli:**

a) **przedmiot kontroli:** bezpieczeństwo teleinformatyczne w pracy zdalnej i mobilnym przetwarzaniu danych,

b) **okres objęty kontrolą:** od 1 stycznia 2022 r. do dnia zakończenia kontroli, z możliwością wykorzystania dowodów sporządzonych przed tym okresem.

**III. Kontrolę przeprowadzili:**

- Marcin Dziurzyński (kierownik zespołu kontrolerów) – główny specjalista w Departamencie Kontroli w Ministerstwie Funduszy i Polityki Regionalnej (dalej: MFiPR),
- Daniel Banasiak – główny informatyk w Departamencie Informatyki w MFiPR,
- Dariusz Pietrzykowski – kierownik Zespołu do spraw Bezpieczeństwa Teleinformatycznego w Departamencie Informatyki w MFiPR,

na podstawie upoważnienia nr: MFiPR/64-UDG/23 z dnia 18.09.2023 r.

**IV. Termin i sposób przeprowadzenia czynności kontrolnych**

Czynności kontrolne przeprowadzono w terminie 29.09 – 15.12.2023 r. w trybie hybrydowym, tj. w trybie zdalnym i „na miejscu" 7.12.2023 r.

Kontrola została przeprowadzona na podstawie art. 6 ust. 3 pkt 1 ustawy z dnia 15 lipca 2011 r. o kontroli w administracji rządowej[1] (dalej: ustawa o kontroli), art. 31 ust. 3 ustawy z dnia 20 lipca 2017 r. o Krajowym Zasobie Nieruchomości[2]

[1] Dz. U. z 2020 r. poz. 224.
[2] Dz. U. z 2023 r. poz. 1054, ze zm.

tel. 22 273 70 10
www. ov. l web fundusze-re ion,
www.funduszeeuropejskie.gov.pl

ul. Wspólna 2/4
00-926 Warszawa

oraz art. 25 ust. 1 pkt 3 lit. b ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne[3].

**V. Ocena skontrolowanej działalności**

Celem kontroli było sprawdzenie prawidłowości zapewnienia bezpieczeństwa teleinformatycznego w pracy zdalnej i mobilnym przetwarzaniu danych.

Kontrolą objęto dwa obszary:

- procedury oraz działania podejmowane w zakresie zapewnienia bezpieczeństwa teleinformatycznego w pracy zdalnej i mobilnym przetwarzaniu danych;
- środki zastosowane do ochrony danych przetwarzanych mobilnie.

Na podstawie ustaleń zawartych w niniejszym projekcie wystąpienia pokontrolnego oraz przyjętego kryterium kontroli[4], **działania podejmowane przez Kierownika jednostki kontrolowanej w badanym zakresie oceniono negatywnie.**

Powyższa ocena wynika z następujących nieprawidłowości stwierdzonych we wszystkich skontrolowanych obszarach:

- niedokonywanie przeglądów systemu zarządzania bezpieczeństwem informacji;
- nieprzeprowadzanie okresowej analizy ryzyka utraty integralności, dostępności lub poufności informacji;
- brak szczegółowych zasad dot. bezpiecznego korzystania z Internetu i poczty elektronicznej oraz brak procedury przeglądu i blokowania kont domenowych oraz pocztowych, które są długotrwale nieużywane, co w istotny sposób zmniejsza bezpieczeństwo pracy przy przetwarzaniu mobilnym i pracy na odległość;
- niestosowanie pełnego szyfrowania dysków twardych komputerów przenośnych, co nie zapewnia zabezpieczenia informacji w sposób uniemożliwiający nieuprawnionemu jej ujawnienie, modyfikacje, usunięcie lub zniszczenie oraz stosowania mechanizmów kryptograficznych w sposób adekwatny do zagrożeń;
- niewdrożenie systemu klasy [redacted] wspierającego zarządzanie telefonami komórkowymi, co stwarza wysokie ryzyko nieuprawnionego ujawnienia, modyfikacji, usunięcia lub zniszczenie informacji;
- nieobsadzenie stanowiska koordynatora systemu zarządzania bezpieczeństwem informacji w okresie od 1.09.2021 r. do 25.07.2022 r.;
- nieprzeprowadzanie cyklicznych, raz na kwartał, kontroli pracy zdalnej w miejscu jej wykonywania przez pracownika;
- brak oświadczeń 34 pracowników KZN (na 76 zatrudnionych) o zapoznaniu się z obowiązującym system zarządzania bezpieczeństwem informacji.

Powyższe nieprawidłowości związane są z naruszeniami rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci

[3] Dz. U. z 2023 r. poz. 57, ze zm.

[4] Jako kryterium kontroli przyjęto legalność.

elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych[5] (dalej: rozporządzenie KRI), a także regulacji wewnętrznych obowiązujących w jednostce kontrolowanej.

Ponadto ustalono, że:

- nie wdrożono zaleceń z audytu bezpieczeństwa informacji dot. wprowadzenia w KZN systemu wspomagającego ochronę danych przed kradzieżą czy przypadkowymi wyciekami oraz zakupu nowego klastra do firewalla;
- działania szkoleniowe nie zapewniały pracownikom uzyskania niezbędnej wiedzy o zagrożeniach dla bezpieczeństwa informacji przetwarzanych w trakcie pracy zdalnej oraz w sposób mobilny.

Mając na względzie, że z pracy zdalnej mogą korzystać co do zasady wszyscy pracownicy KZN[6], którzy wyposażeni są w służbowe komputery przenośne (84 szt.)[7], należy uznać, że stwierdzone nieprawidłowości mogą skutkować znacznym ryzykiem wystąpienia incydentów w zakresie naruszenia bezpieczeństwa informacji.

Z tytułu pełnionego nadzoru za stwierdzone nieprawidłowości odpowiedzialność ponosi Pan Arkadiusz Urban, będący w okresie objętym kontrolą Kierownikiem jednostki kontrolowanej.

Za nieprawidłowości związane z ustanowieniem, wdrożeniem i utrzymywaniem procesów w ramach systemu zarządzania bezpieczeństwem informacji oraz kontrolą pracy zdalnej odpowiedzialność pono[redacted] będący w KZN w okresie objętym kontrolą pełnomocnikiem do spraw SZBI.

## VI. Ustalenia stanu faktycznego

### 1. Ustalenia ogólne

#### 1.1. Kierownik jednostki kontrolowanej

W okresie objętym kontrolą Kierownikiem jednostki kontrolowanej był Pan Arkadiusz Urban, pełniący funkcję prezesa KZN.

#### 1.2. Regulacje prawne w zakresie przedmiotu kontroli

W kontrolowanym zakresie obowiązywały następujące regulacje prawne:

- ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne;
- rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych.

#### 1.3. Regulacje wewnętrzne

W kontrolowanym zakresie w jednostce kontrolowanej obowiązywały następujące regulacje wewnętrzne:

- zarządzenie nr 47/2020 Prezesa Krajowego Zasobu Nieruchomości z dnia 30 października 2020 r. w sprawie aktualizacji systemu zarządzania

[5] Dz. U. z 2017 r. poz. 2247.
[6] Z wyłączeniem pracowników zatrudnionych na stanowisku kierowcy.
[7] Pisemne wyjaśnienia KZN z 11.10.2023 r.

bezpieczeństwem informacji w Krajowym Zasobie Nieruchomości (obowiązujące od 1.11.2020 r.) – dalej: zarządzenie nr 47/2020;

- zarządzenie nr 43a/2023 Prezesa Krajowego Zasobu Nieruchomości z dnia 29 września 2023 r. zmieniające zarządzenie w sprawie aktualizacji systemu zarządzania bezpieczeństwem informacji w Krajowym Zasobie Nieruchomości (obowiązujące od 1.10.2023 r.) – dalej: zarządzenie nr 43a/2023;
- zarządzenie nr 46/2020 Prezesa Krajowego Zasobu Nieruchomości z dnia 30 października 2020 r. w sprawie aktualizacji Polityki Bezpieczeństwa i Ochrony Danych Osobowych w Krajowym Zasobie Nieruchomości (obowiązujące od 1.11.2020 r.) – dalej: zarządzenie nr 46/2020;
- zarządzenie nr 22/2020 Prezesa Krajowego Zasobu Nieruchomości z dnia 25.06.2020 r. w sprawie zasad korzystania i przyznawania do użytkowania służbowych urządzeń mobilnych Krajowego Zasobu Nieruchomości (obowiązujące od 1.07.2020 r.) – dalej: zarządzenie nr 22/2020;
- zarządzenie nr 6/2019 Pełnomocnika do spraw organizacji Krajowego Zasobu Nieruchomości z dnia 21 maja 2019 r. w sprawie ustalenia regulaminu pracy (obowiązujące od 22.05.2019 r.) – dalej: zarządzenie nr 6/2019;
- zarządzenie nr 11/2023 Prezesa Krajowego Zasobu Nieruchomości z dnia 24 marca 2023 r. w sprawie zmiany regulaminu pracy oraz zmiany regulaminu wynagradzania pracowników Krajowego Zasobu Nieruchomości (obowiązujące od 7.04.2023 r.) – dalej: zarządzenie nr 11/2023;
- zarządzenie nr 38/2023 Prezesa Krajowego Zasobu Nieruchomości z dnia 31 sierpnia 2023 r. w sprawie nadania regulaminu pracy zdalnej (obowiązujące od 1.09.2023 r.) – dalej: zarządzenie nr 38/2023;
- zarządzenie nr 10/2019 Pełnomocnika do spraw organizacji Krajowego Zasobu Nieruchomości z dnia 22 lipca 2019 r. w sprawie powołania inspektora ochrony w Biurze Krajowego Zasobu Nieruchomości (obowiązujące od 23.07.2019 r.) – dalej: zarządzenie nr 10/2019;
- zarządzenie nr 21/2022 Prezesa Krajowego Zasobu Nieruchomości z dnia 25 lipca 2022 r. w sprawie powołania inspektora ochrony danych w Biurze Krajowego Zasobu Nieruchomości (obowiązujące od 26.07.2022 r.) – dalej: zarządzenie nr 21/2022.

**1.4. Informacje dodatkowe**

W przedmiocie objętym kontrolą, od czasu przejęcia nadzoru nad KZN przez Ministra Funduszy i Polityki Regionalnej[8], nie wpłynęły do MFiPR skargi lub wnioski w rozumieniu ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego[9].

KZN nie był wcześniej kontrolowany przez MFiPR w tym przedmiocie.

MFiPR nie posiada informacji o kontrolach przeprowadzonych przez inne organy w tym przedmiocie.

[8] Tj. od 1.08.2022 r.

[9] Dz. U. z 2023 r. poz. 775, ze zm.

## 2. Ustalenia szczegółowe

### 2.1. Procedury oraz działania podejmowane w zakresie zapewnienia bezpieczeństwa teleinformatycznego w pracy zdalnej i mobilnym przetwarzaniu danych

#### 2.1.1. Procedury oraz organizacja systemu zarządzania bezpieczeństwem informacji

W KZN ustanowiono system zarządzania bezpieczeństwem informacji[10] (dalej także: SZBI), o czym mowa w § 20 ust. 1 rozporządzenia KRI. SZBI opracowano na podstawie Polskiej Normy PN-ISO/IEC 27001, co wypełnia dyspozycję zawartą w § 20 ust. 3 tego rozporządzenia. W SZBI uwzględniono m.in. politykę oraz organizację systemu zarządzania bezpieczeństwem informacji, zasady bezpieczeństwa informacji oraz bezpieczeństwa teleinformatycznego.

W oparciu o funkcjonujące w KZN regulacje wewnętrzne w zakresie systemu zarządzania bezpieczeństwem informacji ustalono, że:

- dostęp do aktywów informacyjnych jednostki, umożliwiający wykonywanie zadań przez pracowników w trakcie pracy zdalnej, zapewniony był poprzez udostępnienie pracownikom m. in. komputera służbowego (laptopa) wraz z odpowiednim oprogramowaniem oraz telefonu komórkowego z dostępem do Internetu[11],
- ustanowiono procedury bezpieczeństwa teleinformatycznego podczas użytkowania urządzeń mobilnych, w szczególności dotyczące ochrony sprzętu poza siedzibą KZN (w tym sposobu postępowania w przypadku jego kradzieży)[12] oraz zabezpieczania sprzętu poprzez m.in.:
    - szyfrowanie dysków,
    - stosowanie: indywidualnych kont użytkowników zabezpieczonych hasłem spełniającym określone wymagania, blokady ekranu, oprogramowania umożliwiającego połączenie z serwerem KZN tylko poprzez VPN,
    - instalowanie aktualizacji systemowych oraz programu antywirusowego[13],
- ustanowiono procedury dotyczące m.in.: przeglądu SZBI, zarządzania ryzykiem w bezpieczeństwie informacji, działania w przypadku wystąpienia incydentów naruszenia bezpieczeństwa informacji[14].

Ustalono, że w ramach systemu zarządzania bezpieczeństwem informacji nie ustanowiono szczegółowych zasad dot. bezpiecznego korzystania z Internetu i poczty elektronicznej oraz nie przewidziano procedury przeglądu i blokowania kont domenowych oraz pocztowych, które są długotrwale nieużywane. Powyższe

---

[10] Zarządzenie nr 47/2020 oraz zarządzenie nr 43a/2023.

[11] Załącznik nr 6. Bezpieczeństwo Teleinformatyczne do zarządzenia nr 47/2020 (pkt 4. 6) C) oraz § 7 ust. 1 i 2 Regulaminu pracy zdalnej KZN, stanowiącego załącznik do zarządzenia nr 38/2023.

[12] § 5 zarządzenia nr 22/2020.

[13] Załącznik nr 6. Bezpieczeństwo Teleinformatyczne do zarządzenia nr 47/2020 (pkt 4. 1) A i B, pkt 4. 4) A, pkt 4. 10)).

[14] Odpowiednio: załącznik nr 4. Organizacja Systemu Zarządzania Bezpieczeństwem Informacji do zarządzenia nr 47/2020 (pkt 4. 11)), załącznik nr 8. Metodyka Analizy Ryzyka do zarządzenia nr 47/2020, załącznik nr 5. Zasady Bezpieczeństwa Informacji do zarządzenia nr 47/2020 (pkt 4. 10)).

zaniechanie w istotny sposób zmniejsza bezpieczeństwo pracy przy przetwarzaniu mobilnym i pracy na odległość, a tym samym narusza § 20 ust. 2 pkt 8 rozporządzenia KRI. Bezpośrednią odpowiedzialność za to ponosi pełnomocnik do spraw SZBI, który, zgodnie z § 2 ust. 2 pkt 3 zarządzenia nr 47/2020, zobligowany był do zapewnienia, że procesy potrzebne w ramach systemu zarządzania bezpieczeństwem informacji są ustanowione, wdrożone i utrzymywane.

W KZN powołano pełnomocnika do spraw SZBI, którego zadania realizuje administrator systemów informatycznych[15] oraz koordynatora SZBI, którego zadania realizuje inspektor ochrony danych[16].

Administratorowi systemów informatycznych, zatrudnionemu na podstawie umowy o pracę, przypisano szczegółowe odpowiedzialności w zakresie bezpieczeństwa teleinformatycznego[17]. Zadania administratora systemów informatycznych w zakresie wdrażania odpowiednich środków organizacyjnych i technicznych w celu zabezpieczenia danych osobowych, wskazano w polityce bezpieczeństwa i ochrony danych osobowych w KZN[18].

W kontrolowanym okresie zadania związane z obsługą informatyczną w KZN, oprócz administratora systemów informatycznych, wykonywały jeszcze 2 osoby[19].

Ustalono, że w okresie od 1.09.2021 r. do 25.07.2022 r. w KZN był wakat na stanowisku inspektora ochrony danych[20], co skutkowało nieobsadzeniem przez ten okres stanowiska koordynatora SZBI i tym samym naruszeniem postanowień § 3 ust. 1 zarządzenia nr 47/2020.

W KZN wprowadzono regulacje wewnętrze w zakresie pracy zdalnej[21], w których zawarto m.in. postanowienia dotyczące zasad: korzystania z powierzonego pracownikom sprzętu; zabezpieczania otoczenia pracy oraz stanowiska pracy; bezpiecznego logowania. Z pracy zdalnej mogą korzystać wszyscy pracownicy, z wyłączeniem pracowników zatrudnionych na stanowisku kierowcy[22].

W regulacjach wewnętrznych dot. pracy zdalnej przewidziano wykonywanie przez pracodawcę kontroli pracy zdalnej u pracownika w ustalonym miejscu jej świadczenia, w tym w zakresie przestrzegania wymogów bezpieczeństwa i ochrony danych. Ustalono, że administrator systemów informatycznych w KZN[23] nie przeprowadzał cyklicznych, raz na kwartał, kontroli pracy zdalnej w miejscu jej wykonywania przez pracownika[24], do czego obligował go § 16 ust. 4 załącznika nr 1 do zarządzenia nr 11/2023, obowiązującego w okresie 7.04 – 31.08.2023 r.

---

[15] § 2 zarządzenia nr 47/2020.
[16] § 3 zarządzenia nr 47/2020.
[17] Wskazane w SZBI oraz w zakresie obowiązków do umowy o pracę.
[18] Zarządzenie nr 46/2020.
[19] P.S. na podstawie umowy nr 18/DZP/ZO/07/2022 z 23.02.2022 r. (aneksowanej 20.01.2023 r.) oraz D.K. na podstawie: umowy nr 13/DZP/ZO/07/2021 z 29.01.2021 r.; umów o pracę z: 01.02.2022 r., 29.04.2022 r., 29.11.2022 r.; umowy o współpracy z 14.09.2023 r.
[20] Pisemne wyjaśnienia KZN z 15.12.2023 r. Inspektora ochrony danych powołano z dniem 23.07.2019 r. (na podstawie zarządzenia nr 10/2019), a kolejnego – z dniem 26.07.2022 r. (na podstawie zarządzenia nr 21/2022).
[21] Zarządzenie nr 6/2019, zarządzenie nr 11/2023, zarządzenie nr 38/2023.
[22] Zgodnie z § 2 ust. 1 Regulaminu pracy zdalnej KZN, stanowiącego załącznik do zarządzenia nr 38/2023.
[23] Pełniący funkcję pełnomocnika do spraw SZBI.
[24] Pisemne wyjaśnienia KZN z 22.11.2023 r.

W ramach systemu zarządzania bezpieczeństwem informacji wskazano role i odpowiedzialności poszczególnych osób oraz ustanowiono wiele procedur, które wspierają bezpieczeństwo teleinformatyczne podczas użytkowania urządzeń mobilnych oraz pracy zdalnej. Jednakże w ocenie kontrolerów, z uwagi na brak ustanowienia w KZN szczegółowych zasad dot. bezpiecznego korzystania z Internetu i poczty elektronicznej, a także brak procedury przeglądu i blokowania kont domenowych oraz pocztowych, które są długotrwale nieużywane, SZBI posiada istotne słabości w zakresie zapewnienia odpowiedniego poziomu bezpieczeństwa.

### 2.1.2. Wyniki audytu SZBI

W kontrolowanym okresie w KZN przeprowadzono audyt bezpieczeństwa informacji, co wypełnia dyspozycję zawartą w § 20 ust. 2 pkt 14 rozporządzenia KRI.

Audyt został przeprowadzony 8.11.2022 r. przez podmiot zewnętrzny. W żadnym z kryteriów audytu[25] nie sformułowano zastrzeżeń. W wyniku audytu[26] wydano zalecenia dot. m.in. wprowadzenia systemu [redacted] j. systemu wspomagającego ochronę danych przed kradzieżą czy przypadkowymi wyciekami; zakupu nowego klastra do firewalla w celu podniesienia poziomu bezpieczeństwa informacji w jednostce.

W wyniku kontroli na miejscu dokonano badania i ustalono, że na dzień 07.12.2023 r.[27] nie wdrożono żadnego z powyższych zaleceń.

W ocenie kontrolerów brak realizacji przedmiotowych zaleceń wpływa na zmniejszenie poziomu bezpieczeństwa teleinformatycznego w KZN.

### 2.1.3. Przeglądy SZBI oraz okresowa analiza ryzyka

Zgodnie z postanowieniami SZBI przeglądy systemu zarządzania bezpieczeństwem informacji powinny być przeprowadzane w KZN raz w roku i dokumentowane m.in. protokołem, a za ich organizację odpowiada pełnomocnik do spraw SZBI[28].

KZN nie przekazał, pomimo takiego wniosku kontrolerów, dokumentacji potwierdzającej dokonywanie w okresie objętym kontrolą przeglądów systemu zarządzania bezpieczeństwem informacji[29], o czym mowa w § 20 ust. 1 rozporządzenia KRI oraz w Polskiej Normie PN-ISO/IEC 27001, która jest wyznacznikiem dla stwierdzenia zgodności ustanowionych regulacji z wymaganiami tego rozporządzenia, oraz w pkt. 4. 11) Organizacji Systemu Zarządzania Bezpieczeństwem Informacji, dokumencie stanowiącym załącznik nr 4 do zarządzenia nr 47/2020. Kontrolerzy uznają zatem, że brak przekazania do kontroli przedmiotowej dokumentacji wskazuje na nieprzeprowadzanie w KZN przeglądów systemu zarządzania bezpieczeństwem informacji.

---

[25] Kryteria: weryfikacja systemu ochrony i bezpieczeństwa danych, informacji oraz danych osobowych; badanie systemu dokumentacji SZBI w oparciu o wymagania KRI; weryfikacja zabezpieczeń fizycznych pod kątem wymagań UODO; weryfikacja zapisów systemu bezpieczeństwa przetwarzania dla potwierdzenia poziomu bezpieczeństwa informacji; weryfikacja systemów teleinformatycznych, stanu infrastruktury sieciowej i bezpieczeństwa teleinformatycznego; wywiady on-site z pracownikami organizacji.

[26] Protokół z audytu bezpieczeństwa informacji z 1.12.2022 r.

[27] Ustalono w trakcie kontroli na miejscu w siedzibie kontrolowanego.

[28] Załącznik nr 4. Organizacja Systemu Zarządzania Bezpieczeństwem Informacji do zarządzenia nr 47/2020 (pkt 4. 11)).

[29] Pismo kontrolerów z 26.10.2023 r. i pisemna odpowiedź KZN z 6.11.2023 r.

Zgodnie z postanowieniami SZBI za analizę ryzyka odpowiedzialny jest pełnomocnik do spraw SZBI, a ponowna ocena zidentyfikowanego ryzyka nie może być rzadsza niż raz na 12 miesięcy[30]. W KZN, w okresie objętym kontrolą, nie przeprowadzano okresowej analizy ryzyka utraty integralności, dostępności lub poufności informacji[31], co stanowi naruszenie § 20 ust. 2 pkt 3 rozporządzenia KRI.

W ocenie kontrolerów brak przeprowadzania przeglądów SZBI oraz okresowej analizy ryzyka negatywnie wpływa na zapewnienie stałej przydatności, adekwatności i skuteczności systemu zarządzania bezpieczeństwem informacji w KZN.

**2.1.4. Działania szkoleniowe oraz znajomość przez pracowników procedur SZBI**

Kontrolerzy wystąpili do KZN z wnioskami o wskazanie konkretnych działań jakie podjęto w zakresie zapoznawania pracowników z zagrożeniami dla bezpieczeństwa informacji przetwarzanych w trakcie pracy zdalnej oraz w sposób mobilny, ogólnymi zagadnieniami cyberbezpieczeństwa[32], a także przekazanie informacji nt. szkoleń/kursów jakie odbyli pracownicy w powyższym zakresie (wraz z podaniem liczby przeszkolonych pracowników, nazwy szkoleń i ich programów oraz terminów ich przeprowadzenia)[33].

W ramach powyższych wniosków:

- złożono wyjaśnienia, że *„każdy pracownik podejmujący pracę zdalną był informowany o możliwych zagrożeniach przez administratora, w czasie przeglądu służbowego sprzętu i sprawdzeniu jego prawidłowości działania, przed opuszczeniem biura"*[34],
- przekazano dokumentację dot. szkoleń w zakresie:
  - bezpieczeństwa informacji i ochrony danych osobowych (umowa z wykonawcą wraz z opisem przedmiotu zamówienia, który nie wskazuje w sposób jednoznaczny, że zakresem szkolenia były objęte przedmiotowe zagadnienia; e-mail z linkiem do spotkania w aplikacji Microsoft Teams wysłany do kilkunastu pracowników),
  - bezpiecznej pracy zdalnej (skan potwierdzający zdanie testu przez jednego z pracowników KZN),
  - RODO (e-mail z linkiem do bezpłatnego szkolenia wysłany do pracownika KZN)[35].

Przekazane w trakcie kontroli wyjaśnienia oraz niepełna dokumentacja dot szkoleń wskazują, że podejmowane działania nie zapewniały uzyskania przez pracowników niezbędnej wiedzy o zagrożeniach dla bezpieczeństwa informacji przetwarzanych w trakcie pracy zdalnej oraz w sposób mobilny. Powyższe wskazuje też na niewystarczającą realizację zadania dot. nadzorowania szkoleń z zakresu SZBI, które, zgodnie z § 2 ust. 2 pkt 9 zarządzenia nr 47/2020, przypisano do pełnomocnika do spraw SZBI.

[30] Załącznik nr 8. Metodyka Analizy Ryzyka do zarządzenia nr 47/2020 (pkt 4. 2) b).
[31] Pisemne wyjaśnienia KZN z 11.10.2023 r.
[32] Pismo kontrolerów z 26.10.2023 r.
[33] Pisemny wniosek kontrolerów z 7.12.2023 r.
[34] Pisemne wyjaśnienia KZN z 6.11.2023 r.
[35] Pismo KZN z 15.12.2023 r. oraz korespondencja e-mailowa z 15.12.2023 r.

Ustalono, że 34 pracowników KZN nie złożyło oświadczeń o zapoznaniu się z SZBI, co stanowi naruszenie zapisów zawartych w pkt. 4. 2) A Zasad Bezpieczeństwa Informacji, dokumencie stanowiącym załącznik nr 5 do zarządzenia nr 47/2020. Podczas prowadzenia kontroli na miejscu w siedzibie kontrolowanego stwierdzono, że przedmiotowe oświadczenia złożyło 42 pracowników na 76 zatrudnionych.

Ponadto ustalono, że:

- oświadczenia te nie zawierają daty ich złożenia, oprócz jednego z 19.10.2023 r.;
- treść tych oświadczeń odpowiada treści zawartej w załączniku nr 1 do zarządzenia nr 43a/2023, które obowiązywało od 1.10.2023 r.

Podczas kontroli kontrolowany nie przedstawił oświadczeń o zapoznaniu się przez pracowników z SZBI, których wzór[36], różniący się od tego wskazanego w zarządzeniu nr 43a/2023, obowiązywał w okresie od 1.11.2020 r. do 31.09.2023 r.

Powyższe wskazuje na istotne ryzyko w zakresie niewystarczającej znajomości SZBI przez pracowników KZN.

W ocenie kontrolerów działania podejmowane w zakresie uświadamiania pracowników o zagrożeniach dla bezpieczeństwa informacji przetwarzanych w trakcie pracy zdalnej oraz w sposób mobilny, a także zaznajomienia ich z SZBI były niewystarczające.

**W związku ze stwierdzonymi naruszeniami prawa, działalność KZN w obszarze procedur oraz działań podejmowanych w zakresie zapewnienia bezpieczeństwa teleinformatycznego w pracy zdalnej i mobilnym przetwarzaniu danych ocenia się negatywnie.**

**2.2. Środki zastosowane do ochrony danych przetwarzanych mobilnie**

Podczas kontroli na miejscu w siedzibie kontrolowanego potwierdzono, w ramach przeprowadzonego sprawdzenia konfiguracji systemów: operacyjnych, antywirusowych, sporządzania kopii bezpieczeństwa, zarządzających politykami dostępu do zasobów teleinformatycznych oraz inwentaryzacyjnych umożliwiających weryfikację specyfikacji sprzętowo-systemowej każdego komputera w domenie KZN, że:

- dostęp z zewnątrz do wewnętrznych zasobów teleinformatycznych przechowywanych na serwerach w siedzibie KZN możliwy był tylko z komputerów służbowych pracujących w domenie i został zabezpieczony poprzez zastosowanie szyfrowanego kanału VPN;
- dostęp do zasobów przechowywanych w chmurze zabezpieczony był poprzez logowanie domenowe z dodatkową autentykacją w postaci kodu SMS przesyłanego na służbowy telefon komórkowy użytkownika;
- na sprzęcie komputerowym instalowano aktualizacje systemów operacyjnych oraz używano program antywirusowy z aktualnymi sygnaturami wirusów;

[36] Stanowiący załącznik nr 1 do Zasad Bezpieczeństwa Informacji (załącznik nr 5 do zarządzenia nr 47/2020).

- wdrożono mechanizm sporządzania kopii bezpieczeństwa danych (używano stosownego oprogramowania dla środowiska serwerów wirtualnych);
- konta użytkowników nie posiadały uprawnień administratora zezwalających na instalowanie oprogramowania (użytkownicy używali konta domenowego z prawem zwykłego użytkownika);
- na komputerach były skonfigurowane imienne konta użytkowników, a dostęp do kont funkcyjnych ograniczono wskazując imienne konta osób upoważnionych;
- stosowano ustawienia systemowe wymuszające używanie haseł spełniających reguły złożoności;
- stosowano blokadę ekranu w komputerach;
- w zakresie bezpieczeństwa połączeń monitorowano ruch sieciowy pod kątem wystąpienia połączeń niepożądanych (funkcjonowały odpowiednie systemy monitorujące);
- monitorowanie logowań do systemów dziedzinowych realizowane było z wykorzystaniem systemu SEM.

Nie stwierdzono, w okresie objętym kontrolą, wystąpienia incydentów bezpieczeństwa informacji związanych z wykonywaniem pracy zdalnej[37].

Stwierdzono istotną słabość w zakresie zabezpieczenia informacji przetwarzanych w służbowych telefonach komórkowych. Niewdrożenie systemu klasy [redacted] wspierającego zarządzanie telefonami komórkowymi w zakresie monitorowania ich aktywności i ustawień (np. systemowe wymuszenia blokady telefonu przy pomocy kodu PIN)[38] stwarza wysokie ryzyko nieuprawnionego ujawnienia, modyfikacji, usunięcia lub zniszczenia informacji. Stanowi to naruszenie § 20 ust. 2 pkt 9 rozporządzenia KRI.

Ustalono, że niestosowano systemowego, wspieranego dedykowanym narzędziem, pełnego szyfrowania dysków twardych komputerów przenośnych, pomimo że procedury SZBI nakazywały takie działanie[39]. Kontrolujących poinformowano o poczynionych działaniach w celu wdrożenia pełnego szyfrowania dysków, tj. o przygotowaniu odpowiedniej polityki GPO oraz testach rozwiązania w trybie produkcyjnym. Nie zdefiniowano perspektywy czasowej wdrożenia pełnego szyfrowania dysków twardych komputerów przenośnych[40].

Niestosowanie pełnego szyfrowania dysków twardych komputerów przenośnych stanowi naruszenie § 20 ust. 2 pkt 9 oraz § 20 ust. 2 pkt 12 lit. d rozporządzenia KRI, obligujących do zabezpieczenia informacji w sposób uniemożliwiający nieuprawnionemu jej ujawnienie, modyfikację, usunięcie lub zniszczenie oraz do stosowania mechanizmów kryptograficznych w sposób adekwatny do zagrożeń.

---

[37] Pisemne wyjaśnienia KZN z 11.10.2023 r.

[38] Zgodnie z załącznikiem nr 6. Bezpieczeństwo Teleinformatyczne do zarządzenia nr 47/2020 (pkt 4. 1) A), to pracownik ma obowiązek zastosować blokadę ekranu telefonu komórkowego przynajmniej na kod 4 znakowy lub na hasło alfanumeryczne.

[39] Załącznik nr 6. Bezpieczeństwo Teleinformatyczne do zarządzenia nr 47/2020 (pkt 4. 1) A).

[40] Pisemne wyjaśnienia KZN z 11.10.2023 r.

Bezpośrednią odpowiedzialność za powyższe ponosi pełnomocnik SZBI, który, zgodnie z § 2 ust. 2 pkt 3 zarządzenia nr 47/2020, zobligowany był do zapewnienia, że procesy potrzebne w ramach systemu zarządzania bezpieczeństwem informacji są ustanowione, wdrożone i utrzymywane.

**W związku ze stwierdzonymi naruszeniami prawa, działalność KZN w obszarze środków zastosowanych do ochrony danych przetwarzanych mobilnie ocenia się negatywnie.**

## VII. Pozostałe informacje

Do *Projektu wystąpienia pokontrolnego* zostały zgłoszone zastrzeżenia w trybie art. 40 ustawy o kontroli. Zastrzeżenia zostały rozpatrzone.

## VIII. Zalecenia pokontrolne

Biorąc pod uwagę powyższe ustalenia i oceny, na podstawie art. 46 ust. 3 pkt 1 *ustawy o kontroli*, zalecam:

1. Dokonywanie przeglądów systemu zarządzania bezpieczeństwem informacji z zachowaniem terminów i zakresu określonych w regulacji, oraz przeprowadzanie okresowej analizy ryzyka utraty integralności, dostępności lub poufności informacji.
2. Ustanowienie, w ramach systemu zarządzania bezpieczeństwem informacji, szczegółowych zasad dot. bezpiecznego korzystania z Internetu i poczty elektronicznej oraz procedury przeglądu i blokowania kont domenowych oraz pocztowych, które są długotrwale nieużywane.
3. Zapewnienie bezpieczeństwa informacji poprzez pełne szyfrowanie dysków twardych komputerów przenośnych.
4. Przekazanie harmonogramu w zakresie wdrożenia systemu klasy [redacted] wspierającego zarządzanie telefonami komórkowymi.
5. Zapewnienie ciągłości działania na stanowisku koordynatora systemu zarządzania bezpieczeństwem informacji.
6. Przestrzeganie regulacji wewnętrznych w zakresie kontroli pracy zdalnej w miejscu jej wykonywania przez pracownika.
7. Udokumentowanie zapoznania się z obowiązującym system zarządzania bezpieczeństwem informacji, poprzez potwierdzenie tego faktu przez pracownika podpisem i datą.
8. Podjęcie działań w celu wdrożenia zaleceń z audytu bezpieczeństwa informacji dot. wprowadzenia w KZN systemu wspomagającego ochronę danych przed kradzieżą czy przypadkowymi wyciekami oraz zakupu nowego klastra do firewalla.
9. Przeprowadzić szkolenia w celu zapewnienia pracownikom wiedzy o zagrożeniach dla bezpieczeństwa informacji, przetwarzanych w trakcie pracy zdalnej oraz w sposób mobilny.

Na podstawie art. 49 w związku z art. 46 ust. 3 pkt 3 *ustawy o kontroli* uprzejmie proszę Pana Prezesa o przedstawienie, w terminie 30 dni od dnia otrzymania niniejszego dokumentu, informacji o sposobie wykonania zaleceń, wykorzystaniu wniosków lub przyczynach ich niewykorzystania.

Informuję, że zgodnie z art. 48 *ustawy o kontroli* od *Wystąpienia pokontrolnego* nie przysługują środki odwoławcze.

Z poważaniem

z upoważnienia Ministra Funduszy
i Polityki Regionalnej

Wojciech Kijowski

Dyrektor Generalny

/podpisano elektronicznie/