NAJWYŻSZA IZBA KONTROLI
Delegatura w Olsztynie

LOL.410.017.02.2021

Mariusz Pawłowski
Dyrektor Izby Administracji Skarbowej w Olsztynie
Izba Administracji Skarbowej w Olsztynie
Al. Marszałka J. Piłsudskiego 59A
10-950 Olsztyn

WYSTĄPIENIE POKONTROLNE

P/21/081 - Bezpieczeństwo informacji w pracy na odległość i mobilnym przetwarzaniu danych

NAJWYŻSZA IZBA KONTROLI
Delegatura w Olsztynie
ul. Artyleryjska 3e, 10-165 Olsztyn
T +48 89 678 82 00, F +48 89 678 82 30
lol@nik.gov.pl

I. Dane identyfikacyjne

Jednostka kontrolowana	Izba Administracji Skarbowej w Olsztynie, Al. Marszałka J. Piłsudskiego 59A, 10-950 Olsztyn (dalej: IAS lub Izba)
Kierownik jednostki kontrolowanej	Mariusz Pawłowski, Dyrektor Izby Administracji Skarbowej w Olsztynie, od 9 stycznia 2018 r. (dalej: Dyrektor)
Zakres przedmiotowy kontroli	1. Organizacja bezpieczeństwa informacji. 2. Wdrożone i stosowane rozwiązania organizacyjne i techniczne zapewniające bezpieczeństwo informacji w pracy zdalnej.
Okres objęty kontrolą	Lata 2020 – 2021 (do zakończenia kontroli[1]) z uwzględnieniem zdarzeń wcześniejszych, jeżeli miały one wpływ na kontrolowane obszary działalności.
Podstawa prawna podjęcia kontroli	Art. 2 ust. 1 ustawy z dnia 23 grudnia 1994 r. o Najwyższej Izbie Kontroli[2]
Jednostka przeprowadzająca kontrolę	Najwyższa Izba Kontroli Delegatura w Olsztynie
Kontroler	Sebastian Helbrecht, starszy inspektor kontroli państwowej, upoważnienie do kontroli nr LOL/104/2021 z 6 września 2021 r.

(akta kontroli str. 1-2)

II. Ocena ogólna[3] kontrolowanej działalności

OCENA OGÓLNA

Najwyższa Izba Kontroli ocenia pozytywnie działania Izby mające na celu prawidłowe wykonywanie zadań w zakresie zapewnienia bezpieczeństwa informacji w pracy na odległość i mobilnym przetwarzaniu danych.

Uzasadnienie oceny ogólnej

Izba Administracji Skarbowej właściwie realizowała zadania określone w rozporządzeniu 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[4]. Funkcjonujący w Izbie System Zarządzania Bezpieczeństwem Informacji (dalej: SZBI), został opracowany na podstawie Polskiej Normy PN-ISO/IEC 27001, zawierał reguły, procedury i zasady, według których Izba zarządzała i udostępniała swoje zasoby informacji. Zgodnie z art. 37 ust. 1 Rozporządzenia 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)[5], wyznaczono inspektora ochrony danych (dalej: IOD). Osoba wyznaczona na stanowisko IOD spełniała wymagania określone w art. 37 ust 5 RODO. W celu zapewnienia ciągłości działania Izby, wprowadzono system pracy zdalnej, a opracowany SZBI zapewniał bezpieczeństwo informacji w trakcie jej wykonywania.

[1] 22 listopada 2021 r.
[2] Dz. U. z 2020 r. poz. 1200, ze zm., dalej: ustawa o NIK.
[3] Najwyższa Izba Kontroli formułuje ocenę ogólną jako ocenę pozytywną, ocenę negatywną albo ocenę w formie opisowej.
[4] Dz.U. z 2017 r. poz. 2247, dalej: rozporządzenie KRI.
[5] Dz. Urz. UE L z 2016 r. poz. 119, dalej: RODO.

III. Opis ustalonego stanu faktycznego oraz oceny cząstkowe[6] kontrolowanej działalności

OBSZAR

1. Organizacja bezpieczeństwa informacji

Opis stanu faktycznego

1.1. W Izbie opracowano, ustanowiono i wdrożono System Zarządzania Bezpieczeństwem Informacji stosownie do §20 ust. 1 rozporządzenia 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.

Zarządzenie Dyrektora z 11 lipca 2018 r.[7] określało reguły, procedury i zasady, według których Izba zarządza i udostępnia swoje zasoby informacji. Zarządzenie to określało m.in. zasady postępowania z nośnikami, zarządzania uprawnieniami użytkowników, wynoszenia aktywów, bezpieczeństwa sprzętu i aktywów poza siedzibą, pozostawiania sprzętu bez opieki, zabezpieczenia przed szkodliwym oprogramowaniem, zabezpieczenia sieci, przesyłania informacji, zabezpieczenia wiadomości w formie elektronicznej oraz zarządzania incydentami związanymi z bezpieczeństwem informacji. Integralną część zarządzenia stanowiły trzy procedury, tj.: Polityka Bezpieczeństwa Informacji (dalej: PBI), Polityka Ochrony Danych Osobowych (dalej: PODO) oraz Instrukcja Zarządzania Systemami Informatycznymi (dalej: IZSI).

(akta kontroli str. 3-4)

1.2. Zarządzenie SZBI zawierało strukturę zarządzania bezpieczeństwem informacji, zgodnie z którą przypisano odpowiedzialność za poszczególne obszary, które mają wpływ na bezpieczeństwo informacji, tj. analizę ryzyka, analizę incydentów, aktualizację zasad i procedur. Dyrektor Izby jako administrator danych osobowych (dalej: ADO) sprawował nadzór nad bezpieczeństwem informacji, zarządzał i nadzorował ustanowienie, wdrażanie i monitorowanie SZBI w Izbie. Rolę administratora sieci informatycznej (dalej: ASI) pełniła wyznaczona przez Dyrektora osoba z Wydziału Informatyki, wykonująca czynności związane z administrowaniem i monitorowaniem systemu oraz zapewniająca jego bezpieczną eksploatację. Od 1 stycznia 2021 r., zgodnie z zarządzeniem Ministra Finansów, Funduszy i Polityki Regionalnej[8], zadania z zakresu IT zostały przekazane do realizacji Centrum Informatyki Resortu Finansów. Zgodnie z zarządzeniem SZBI, powołano zespół ds. analizy ryzyka w obszarze bezpieczeństwa informacji w IAS w Olsztynie[9]. Do jego zadań należało dokonywanie przeglądu podatności, zagrożeń i ryzyk oraz skuteczności mechanizmów zabezpieczających. Komórka audytu wewnętrznego, nie rzadziej niż raz w roku przeprowadzała audyt bezpieczeństwa informacji w zakresie funkcjonowania SZBI zgodnie z aktualnym rozporządzeniem KRI[10].

(akta kontroli str. 3-69, 75-83)

---

[6] Oceny cząstkowe to oceny działalności w poszczególnych obszarach badań kontrolnych. Ocena cząstkowa może być sformułowana jako ocena pozytywna, ocena negatywna albo ocena w formie opisowej.

[7] Zarządzenie nr 27/2018 Dyrektora IAS w Olsztynie z dnia 11 lipca 2018 r. w sprawie wprowadzenia SZBI w IAS w Olsztynie i podległych urzędach (dalej: zarządzenie SZBI).

[8] Zarządzenie Ministra Finansów, Funduszy i Polityki Regionalnej z dnia 26 listopada 2020 r. zmieniające zarządzenie w sprawie organizacji Krajowej Informacji Skarbowej, izby administracji skarbowej, urzędu skarbowego, urzędu celno-skarbowego i Krajowej Szkoły Skarbowości oraz nadania im statutów oraz zarządzenie zmieniające zarządzenie w sprawie organizacji Krajowej Informacji Skarbowej, izby administracji skarbowej, urzędu skarbowego, urzędu celno-skarbowego i Krajowej Szkoły Skarbowości oraz nadania im statutów.

[9] Decyzja nr 94/2019 z 17 maja 2019 r., decyzja nr 137/2020 z 2 września 2020 r.

[10] Wieloosobowe stanowisko audytu wewnętrznego przeprowadziło audyt koordynowany w obszarze informatyka w roku 2020.

1.3. Zgodnie z art. 37 ust. 1 rozporządzenia RODO, w Izbie wyznaczono IOD[11], który posiadał kwalifikacje do pełnienia tej funkcji, wskazane w art. 37 ust. 5 rozporządzenia RODO. Zakres przypisanych inspektorowi ochrony danych zadań był zgodny z katalogiem czynności określonych w art. 39 RODO. Regulamin organizacyjny Izby uwzględniał stanowisko IOD i gwarantował niezależność jego działań poprzez bezpośrednią podległość Dyrektorowi Izby. Zgodnie z zarządzeniem SZBI, audyt zgodności ochrony danych osobowych dokonywany był przez IOD, a jego wyniki zawierano w sprawozdaniu rocznym przedkładanym Dyrektorowi.

(akta kontroli str. 70-74)

1.4. W Izbie opracowano zasady postępowania z nośnikami, określono je w regulacjach wewnętrznych w załącznikach do IZSI. Były to trzy procedury: procedura zarządzania nośnikami informacji, procedura bezpiecznej eksploatacji komputerów przenośnych i procedura zabezpieczenia danych na urządzeniach przenośnych i wymiennych nośnikach informacji. Wdrożone procedury dotyczyły m.in. bezpiecznego wycofywania nośników, które nie będą dłużej wykorzystywane oraz ochrony przed nieuprawnionym dostępem, nadużyciem oraz utratą integralności podczas transportu nośników zawierających informacje, stosowanych mechanizmów zapewniających poufność (ochrona fizyczna nośnika oraz mechanizmy kryptograficzne pozwalające zaszyfrować dane na nim zawarte).

(akta kontroli str. 3-4, 49-60)

1.5. Zarządzenie SZBI zawierało zasady wynoszenia aktywów (sprzęt, nośniki, oryginały dokumentów, kopie dokumentów). Zgodnie z tymi zasadami nośniki zawierające dane wrażliwe mogły być wyniesione poza IAS jedynie za zgodą IOD, oraz musiały być zaszyfrowane. W Izbie prowadzono aktualny rejestr nośników służących do przechowywania informacji z przypisaniem odpowiedzialności za dany nośnik.

(akta kontroli str. 3-4, 49-60)

1.6. Zarządzenie SZBI zawierało zasady bezpieczeństwa informacji przesyłanych wewnątrz organizacji i wymienianych z podmiotami zewnętrznymi. PODO zawierało zapisy dotyczące opracowanych technicznych środków ochrony (m.in. strefy bezpieczeństwa, monitoring wizyjny, zasady dostępu do kluczy, ochrona fizyczna dokumentów), organizacyjnych środków ochrony (m.in. opracowane polityki i procedury, upoważnienia) oraz środków ochrony logicznej (m.in. kontrola dostępu do sieci, projektowanie czynności przetwarzania, minimalizacja dostępu). Regulacje w IZSI określały procedurę bezpieczeństwa sieci teleinformatycznych, procedurę zabezpieczenia przed działalnością nieuprawnionego oprogramowania oraz procedurę korzystania z usług Internetu i poczty elektronicznej. Zarządzenie Dyrektora Izby[12] oraz procedura IZSI określały sposób zdalnego dostępu do zasobów, zgodnie z którym można go było uzyskać jedynie na sprzęcie służbowym. Urządzenia musiały zostać podłączone do domeny lub posiadać dedykowane narzędzia uwierzytelniające (tokeny RSA, Google Authenticator). Uzyskanie zdalnego dostępu do systemów informacyjnych Izby wymagało nadania pracownikowi stosownych uprawnień.

(akta kontroli str. 3-60)

1.7. W Izbie określono zasady zarządzania incydentami związanymi z bezpieczeństwem informacji. IZSI zawierała procedurę zabezpieczenia przed

[11] Decyzja nr 144/2018 Dyrektora IAS z 29 maja 2018 r. w sprawie wyznaczenia IOD w IAS w Olsztynie, Decyzja nr 184/2020 Dyrektora IAS z 2 listopada 2020 r. w sprawie wyznaczenia IOD w IAS w Olsztynie.

[12] Zarządzenie nr 49/2017 Dyrektora IAS w Olsztynie z 15 marca 2017 r. w sprawie wprowadzenia w IAS w Olsztynie zasad korzystania z poczty elektronicznej z uwzględnieniem zdalnego dostępu z sieci publicznej.

działalnością nieuprawnionego oprogramowania, opisywała ona zasady mające zapobiegać i wykrywać obecność szkodliwego oprogramowania. Regulacje te określały m.in. sposób zgłaszania incydentów, otwarty katalog zdarzeń wymagających zgłoszenia oraz określały osoby odpowiedzialne i ich role. Zadaniem ASI było m.in. aktualizacja oprogramowania, monitorowanie jego prawidłowości i skuteczności jego działania oraz raportowanie IOD podjętych czynności mających na celu usunięcie złośliwego kodu. W Izbie prowadzono ewidencję incydentów bezpieczeństwa teleinformatycznego w IAS. W PBI zawarto instrukcję postępowania w sytuacji naruszenia bezpieczeństwa, określała ona zasady postępowania w przypadku zaistnienia lub podejrzenia wystąpienia sytuacji naruszenia bezpieczeństwa informacji przetwarzanych w Izbie w systemach informatycznych oraz w formie papierowej. Ustalono w niej definicję naruszenia bezpieczeństwa informacji, opis postępowania w przypadku wystąpienia incydentu oraz raportowanie analizy skutków wystąpienia incydentów i opracowania zaleceń mających na celu podniesienia bezpieczeństwa systemu zabezpieczeń.

(akta kontroli str. 3-60, 84-85)

1.8. W Izbie opracowano i wdrożono regulamin pracy zdalnej[13] oraz umożliwiono w uzasadnionych przypadkach ustalenie indywidualnego rozkładu czasu pracy pracownikom Izby[14]. Indywidualny rozkład czasu pracy polegał m.in. na wykonywaniu pracy w danym dniu roboczym częściowo w siedzibie jednostki, a następnie częściowo w ramach pracy zdalnej bądź naprzemiennie w ramach pracy zdalnej połączonej z dyżurami w siedzibie urzędu. W regulaminie pracy zdalnej określono zasady jej wykonywania, m.in. formę nadzoru przełożonego nad pracą pracownika, metody i kanały komunikacji, sposób i formę przekazywania poleceń i odbioru wyników pracy, metody akceptacji przygotowanych projektów dokumentów i wykonania innych przydzielonych zadań. Ponadto w Izbie, zarządzeniem nr 31/2019 z 6 czerwca 2019 r. zmieniającym Regulamin pracy wprowadzano możliwość wykonywanie pracy w formie telepracy.

(akta kontroli str. 89-109)

1.9. W okresie objętym kontrolą pracownicy Izby uczestniczyli w szkoleniach dotyczących ochrony danych osobowych (15 osób w 2020 r. i 12 w 2021 r.) oraz szkolenia dotyczące bezpieczeństwa teleinformatycznego (72 osoby w 2020 r.). Pracownicy Izby zapoznawali się z regulacjami wewnętrznymi dotyczącymi bezpieczeństwa informacji za pomocą systemu Qasystent[15]. Przy wykonywaniu pracy zdalnej, pracownicy Izby przedkładali podpisane wnioski dotyczące m.in. wykorzystywania komputera do wykonywania pracy zdalnej, o pobranie akt do wykonywania pracy zdalnej. W przedmiotowych wnioskach znajdowało się oświadczenie o zapoznaniu się oraz zrozumieniu przepisów o ochronie informacji i zobowiązanie do przyszłego ich stosowania.

(akta kontroli str. 89-91, 110)

1.10. W okresie kontrolowanym nie wprowadzano nowych i nie modyfikowano istniejących procedur i zasad SZBI. Ostatnia aktualizacja zarządzenia SZBI miała miejsce 25 maja 2018 r. Stosownie do zapisów § 15 Polityki Bezpieczeństwa Informacji będącej jednym z elementów SZBI w Izbie Administracji Skarbowej

[13] Zarządzenie nr 25/2020 Dyrektora IAS w Olsztynie z 3 kwietnia 2020 r. w sprawie działania IAS w Olsztynie wraz z podległymi urzędami w związku z wprowadzeniem od dnia 20 marca 2020 r. do odwołania na obszarze RP stanu epidemii wywołanego zakażeniami wirusem SARS-CoV-2, następnie Zarządzenie nr 49/2021 Dyrektora IAS z 30 lipca 2021 r. w sprawie działania IAS w Olsztynie wraz z podległymi urzędami w stanie epidemii wywołanej chorobą zakaźną.

[14] Zmiana do Regulaminu pracy (Zarządzenie Nr 59/2020 z 6 listopada 2020 r.).

[15] Obowiązek nałożony Zarządzeniem nr 2/2017 Dyrektora IAS w Olsztynie z 1 marca 2017 r. w sprawie ustalenia zasad opracowywania i nadzorowania aktów prawa wewnętrznego w IAS w Olsztynie.

w Olsztynie i podległych urzędach, Dyrektor Izby mógł powołać zespół ds. SZBI, do którego zadań należałoby m.in. dokonywanie okresowych przeglądów i aktualizacji dokumentacji bezpieczeństwa informacji. W okresie objętym kontrolą nie powołano takiego zespołu.

Dyrektor wyjaśnił, że z uwagi na potrzebę szerszego zakresu analizy ryzyka w obszarze bezpieczeństwa informacji powołano Zespół ds. analizy ryzyka w obszarze bezpieczeństwa informacji w Izbie, do zadań którego należało w szczególności prowadzenie ciągłej analizy ryzyka oraz zadania które miałby realizować Zespół ds. SZBI wskazany w PBI. Niezasadnym byłoby zatem równoczesne prowadzenie prac przez dwa zespoły o tożsamych zadaniach i takim samym składzie osobowym, ponadto komórka audytu wewnętrznego co roku przeprowadza audyt bezpieczeństwa informacji w zakresie funkcjonowania SZBI. Brak aktualizacji zarządzenia SZBI spowodowane było wprowadzeniem Polityki Ochrony Danych Osobowych w Ministerstwie Finansów oraz jednostkach podległych i nadzorowanych przez Ministra Finansów, Funduszy i Polityki Regionalnej, jednakże nie opracowano załączników stanowiących integralną część dokumentu, dotyczą one kwestii unormowanych w istniejącym już SZBI w IAS w Olsztynie, a także w poszczególnych izbach administracji skarbowej w kraju. Celem zachowania jednolitości opracowań prawnych i uniknięcia odmiennego uregulowania tych samych zagadnień, zasadnym wydaje się powstrzymanie działań do czasu zakończenia prac ze strony Ministerstwa Finansów.

(akta kontroli str. 3-4, 111-114)

Stwierdzone nieprawidłowości

W działalności kontrolowanej jednostki w przedstawionym wyżej zakresie nie stwierdzono nieprawidłowości.

OCENA CZĄSTKOWA

Najwyższa Izba Kontroli ocenia pozytywnie działalność kontrolowanej jednostki w zbadanym zakresie. Opracowano oraz wdrożono SZBI, zawierający m.in. Politykę Bezpieczeństwa Informacji. W IAS powołano inspektora ochrony danych, spełniającego wymagania określone dla osób, które mogą pełnić tę funkcję. Zapoznano również pracowników z przyjętymi zasadami bezpieczeństwa informacji.

OBSZAR

2. Wdrożone i stosowane rozwiązania organizacyjne i techniczne mające na celu zapewnienie bezpieczeństwa informacji w pracy zdalnej.

Opis stanu faktycznego

2.1. W okresie objętym kontrolą w Izbie:

- 268 pracowników w 2020 r. i 249 w 2021 r. wykonywało pracę na podstawie polecenia pracy zdalnej z inicjatywy pracodawcy,
- 20 pracowników w 2020 r. i 28 w 2021 r. wykonywało pracę zdalną na podstawie polecenia pracy zdalnej z wniosku pracownika,
- 17 pracowników w 2020 r. i 20 w 2021 r. wykonywało pracę zdalną podczas kwarantanny,
- trzech pracowników w 2020 r. i dziewięciu w 2021 r. pracowników wykonywało pracę zdalną podczas izolacji.

(akta kontroli str. 115)

2.2. Pracownicy Izby zapoznawali się z zasadami obejmującymi zapewnienie bezpieczeństwa informacji oraz innymi wdrożonymi dokumentami wewnętrznymi za pomocą systemu Qasystent, obowiązek ten nałożony został Zarządzeniem nr 2/2017 Dyrektora IAS w Olsztynie z 1 marca 2017 r. w sprawie ustalenia zasad opracowywania i nadzorowania aktów prawa wewnętrznego w IAS w Olsztynie.

(akta kontroli str. 3-4)

2.3. W badanym okresie, w ramach wykonywania pracy zdalnej:
- 189 pracowników w 2020 r. i 168 w 2021 r. pracowników wykorzystywało urządzenia teleinformatyczne pracodawcy (komputer, tablet lub smartfon - w szerszym zakresie niż komunikacja głosowa),
- 29 pracowników w 2020 r. i 26 w 2021 r. korzystało ze służbowych telefonów komórkowych tylko do komunikacji głosowej,
- 67 pracowników w 2020 r. i 40 w 2021 r. było wyposażonych w służbowy nośnik danych (np. pendrive lub dysk zewnętrzny),
- 38 pracowników w 2020 r. i trzech w 2021 r. korzystało z prywatnego urządzenia teleinformatycznego (komputer, tablet lub smartfon - w szerszym zakresie niż komunikacja głosowa),
- 199 pracowników w 2020 r. i 160 w 2021 r. korzystało z prywatnych telefonów komórkowych,
- 32 pracowników w 2020 r. i 23 w 2021 r. wykonywało pracę zdalną bez wykorzystania urządzeń teleinformatycznych.

Analiza realizacji obowiązków losowo wybranych 40 pracowników Izby wykonujących pracę zdalną w poszczególnych latach objętych kontrolą wykazała m.in., że:
- 30 pracowników wykorzystywało urządzenia teleinformatyczne (komputery) pracodawcy,
- wszyscy pracownicy wyposażeni w służbowy sprzęt komputerowy uzyskali zgodę na jego wynoszenie poza siedzibę Izby,
- każdy z pracowników pracujący zdalnie na służbowym komputerze miał nadane uprawnienia zdalnego dostępu do systemów teleinformatycznych Izby,
- ośmioro pracowników korzystających z kserokopii i oryginałów dokumentacji posiadała zgodę na wynoszenie tych danych z Izby,
- dwóch pracowników wykonywało pracę zdalną przy użyciu prywatnego sprzętu komputerowego, była to m.in. analiza strony internetowej KAS, analiza przepisów prawa, korzystanie z ogólnodostępnych portali w celu podniesienia wiedzy.

(akta kontroli str. 116-122)

2.4. Wszystkie komputery (stacje robocze oraz laptopy) pracujące w sieci LAN budynku IAS Olsztyn podłączone były do jednej domeny. Czynności jakie dany użytkownik mógł wykonać na swoim komputerze były zależne od tego do jakiej grupy został przypisany w domenie, np.: aby można było zainstalować dowolne oprogramowanie należało być członkiem grupy administratorów.
Przeprowadzone oględziny komputera przenośnego wykorzystywanego do pracy zdalnej wykazały, że:
- dysk stały komputera był zaszyfrowany,
- zalogowany użytkownik systemu informatycznego nie należał do grupy „administratorzy" i nie posiadał uprawnień do instalowania programów i aplikacji,
- przy próbie takiej instalacji w systemie Windows pojawiał się monit o podanie poświadczeń użytkownika z uprawnieniami administratora.

W przypadku, gdy dane, na których wykonywana była praca, przechowywano na urządzeniach przenośnych (np. pamięć USB), były one szyfrowane i chronione hasłem, by zapewnić odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem.

(akta kontroli str. 123-126)

2.5. W Izbie, zgodnie z zarządzeniem SZBI, zdalny dostęp do systemów informatycznych Izby oraz służbowej poczty elektronicznej możliwy był jedynie na sprzęcie komputerowym udostępnionym przez pracodawcę. Pracownicy Izby

podczas wykonywania czynności służbowych w formie pracy zdalnej wykonywali niektóre zadania przy pomocy prywatnego sprzętu komputerowego. Podczas wykonywania tych obowiązków, zobowiązani byli do postępowania zgodnie z SZBI. Czynności jakie realizowano przy pomocy prywatnego sprzętu komputerowego to m.in. analizy stron internetowych, czy korzystanie z ogólnodostępnych aktów prawnych.

(akta kontroli str. 3-4, 117-122)

2.6. Pracownicy IAS wykonujący pracę zdalną pobierali z jednostki oryginały, kserokopie oraz skany dokumentów niezbędne do wykonywania pracy. Przy pobieraniu dokumentacji papierowej sporządzano protokół pobrania akt, który zawierał takie informacje jak uzasadnienie pobrania dokumentacji w wersji papierowej, miejsce przetwarzania i określenie sposobu zabezpieczenia danych, oświadczenie o zapoznaniu się z zasadami i obowiązkami w zakresie ochrony informacji, potwierdzenie pobrania i zwrotu akt.

(akta kontroli str. 117-122, 127-128)

2.7. W Izbie monitorowano i nadzorowano pracę zdalną wykonywaną przez pracowników. Analiza dokumentacji pracy zdalnej dla 40 pracowników wykazała m.in., że wszyscy pracownicy przekazywali ewidencję wykonywanych przez siebie czynności zgodnie z ustalonymi standardami.

W okresie wykonywania pracy zdalnej przez pracowników Izby, nie zgłoszono incydentów związanych z bezpieczeństwem informacji w związku z jej wykonywaniem. Monitorowanie i nadzorowanie wykonywania pracy zdalnej w zakresie bezpieczeństwa informacji odbywało się m.in. poprzez przeglądy dostępów i uprawnień faktycznie posiadanych przez pracowników z uprawnieniami wymaganymi do realizacji zadań zgodnie z zakresami obowiązków, oraz weryfikowanie upoważnień pracowników w celu nadania uprawnień zdalnego dostępu do systemów teleinformatycznych Izby.

(akta kontroli str. 129-130)

Stwierdzone nieprawidłowości

W działalności kontrolowanej jednostki w przedstawionym wyżej zakresie nie stwierdzono nieprawidłowości.

OCENA CZĄSTKOWA

Najwyższa Izba Kontroli ocenia pozytywnie działalność kontrolowanej jednostki w zbadanym zakresie. Podczas pracy zdalnej stosowano regulacje i procedury określone w SZBI. Stosowano rozwiązania techniczne i technologiczne podnoszące poziom bezpieczeństwa informacji. Zapoznano pracowników z zasadami zapewnienia bezpieczeństwa informacji w wykonywaniu pracy zdalnej.

IV. Uwagi i wnioski

W związku z niestwierdzeniem nieprawidłowości, Najwyższa Izba Kontroli nie formułuje uwag ani wniosków pokontrolnych.

V. Pozostałe informacje i pouczenia

Wystąpienie pokontrolne zostało sporządzone w dwóch egzemplarzach; jeden dla kierownika jednostki kontrolowanej, drugi do akt kontroli.

Prawo zgłoszenia zastrzeżeń

Zgodnie z art. 54 ustawy o NIK kierownikowi jednostki kontrolowanej przysługuje prawo zgłoszenia na piśmie umotywowanych zastrzeżeń do wystąpienia pokontrolnego, w terminie 21 dni od dnia jego przekazania. Zastrzeżenia zgłasza się do dyrektora Delegatury NIK w Olsztynie. Prawo zgłaszania zastrzeżeń, zgodnie z art. 61b ust. 2 ustawy o NIK, nie przysługuje do wystąpienia pokontrolnego zmienionego zgodnie z treścią uchwały w sprawie zastrzeżeń.

Olsztyn, 24 listopada 2021 r.

Najwyższa Izba Kontroli
Delegatura w Olsztynie
Dyrektor
z up.
Piotr Wanic
Wicedyrektor

Kontroler
Sebastian Helbrecht
starszy inspektor kontroli państwowej

.....
podpis

.....
podpis