DYREKTOR
IZBY ADMINISTRACJI SKARBOWEJ
W GDAŃSKU

2201-IWW.0920.1.2025

WYSTĄPIENIE POKONTROLNE

Izba Administracji Skarbowej w Gdańsku

I. Dane identyfikacyjne kontroli

Temat kontroli
Ocena zasadności przetwarzania przez pracowników danych uzyskanych za pośrednictwem systemów informatycznych

Kontrolowana komórka organizacyjna Izby Administracji Skarbowej w Gdańsku
Wydział Audytu Środków Pochodzących z Budżetu UE oraz Niepodlegających Zwrotowi Środków z Pomocy Udzielanej przez Państwa Członkowskie EFTA (ICE)

Adres: ul. Żaglowa 2, 80-560 Gdańsk

Kierownik komórki kontrolowanej
Pani Elżbieta Drogoś, Naczelnik Wydziału od 1.01.2023 r.

Kontrolerzy
Maria Kubińska-Matciak - główny ekspert skarbowy – koordynator kontroli,
Wiktor Lipiński – ekspert skarbowy,
działający na podstawie upoważnienia Nr 2201-IWW.0920.1.2025 wydanego przez Dyrektora Izby Administracji Skarbowej w Gdańsku dnia 29.01.2025 r.

Data rozpoczęcia czynności kontrolnych
5.02.2025 r.

Data zakończenia czynności kontrolnych
29.04.2025 r.

Podstawa prawna prowadzenia kontroli:
§ 2 instrukcji w sprawie szczegółowych zasad przeprowadzania kontroli wewnętrznej w komórkach organizacyjnych Izby Administracji Skarbowej w Gdańsku[1].

Okres objęty kontrolą
01.07.2024 r. – 31.12.2024 r. Badaniem zostały objęte również zdarzenia i dokumenty wcześniejsze lub późniejsze, gdy miały związek z przedmiotem kontroli.

Zakres przedmiotowy kontroli

Zakres badania obejmuje następujące zagadnienia kontroli:

1. Organizacja pracy kontrolowanej komórki w zakresie korzystania z systemów informatycznych i nadzór nad prawidłowością wykorzystania danych z systemów informatycznych w ramach kontroli funkcjonalnej;
2. Wykorzystanie systemów informatycznych do celów służbowych.

[redacted]

II. Ocena kontrolowanej działalności

Ocena ogólna

Działania komórki kontrolowanej Wydział Audytu Środków Pochodzących z Budżetu UE oraz Niepodlegających Zwrotowi Środków z Pomocy Udzielanej przez Państwa Członkowskie EFTA (ICE) Izby Administracji Skarbowej w Gdańsku w badanym zakresie oceniono **negatywnie.**

Uzasadnienie oceny ogólnej

Decydujący wpływ na ocenę miał zidentyfikowany incydent bezpieczeństwa informacji oraz nieprawidłowości opisane w części III.1. Szczegółowe uzasadnienie oceny ogólnej stanowią poniższe uwagi dotyczące kontrolowanych zagadnień.

III. Opis ustalonego stanu faktycznego

III.1 Zagadnienie <u>pierwsze</u> z zakresu badania: Organizacja pracy kontrolowanej komórki w zakresie korzystania z systemów informatycznych i nadzór nad prawidłowością wykorzystania danych z systemów informatycznych w ramach kontroli funkcjonalnej**.**

Opis stanu faktycznego

Bezpośredni nadzór nad pracą komórki sprawował Naczelnik Wydziału, pani Elżbieta Drogoś;

Zgodnie ze strukturą organizacyjną Izby Administracji Skarbowej w Gdańsku, Wydział ICE umiejscowiony był w pionach:

1. w okresie od 1.07.2024 r. do 31.07.2024 r. w Pionie Poboru i Egzekucji oraz Kontroli Cła i Audytu (IZPEC), nadzór nad pionem sprawował IV Zastępca Dyrektora, pan Dariusz Jankowiak,
2. w okresie od 1.08.2024 r. do 31.12.2024 r. w Pionie Kontroli, Cła i Audytu (IZPC), nadzór nad pionem sprawował III Zastępca Dyrektora, pan Tomasz Nazarowski.

Zgodnie z wyjaśnieniami Naczelnika ICE z 13.02.2025 r., osobami wyznaczonymi do zastępowania Naczelnika Wydziału są:

- ✓ B.K. - główny ekspert skarbowy, jako pierwsza osoba zastępująca,
- ✓ B.C. - główny ekspert skarbowy, jako druga osoba zastępująca - w przypadku nieobecności pierwszej osoby zastępującej,

W przypadku nieobecności ww. osób, Naczelnik Wydziału wskazuje osobę zastępującą spośród pozostałych pracowników ICE (co do zasady spośród głównych ekspertów skarbowych).

Ponadto, w przypadku nieobecności Naczelnika Wydziału ustawiany jest autoresponder poczty elektronicznej (zarówno dla nadawców z organizacji jak i spoza niej), w którym wskazany jest termin nieobecności Naczelnika Wydziału, osoba go zastępująca i kontakt do tej osoby (e-mail oraz nr telefonu).

[Dowód: pismo–SZD, UNP: 2201-25-027464]

Na dzień 1.07.2024 r. w komórce zatrudnionych było 28 pracowników, natomiast na 31.12.2024 r. – 29 pracowników.
W kontrolowanym okresie pracę w Wydziale ICE podjęło 3 nowych pracowników: J.B. – 2.09.2024 r. (wcześniej, do 31.01.2022 r. była zatrudniona w Pomorskim Urzędzie Celno-Skarbowym w Gdyni), A.K. i A.M. – 5.11.2024 r.
Dwóch pracowników zostało przeniesionych do innych komórek/urzędów.

Do zadań komórki należy miedzy innymi:

- ✓ wykonywanie audytu i kontroli środków pochodzących z budżetu UE oraz niepodlegających zwrotowi środków z pomocy udzielanej przez państwa członkowskie EFTA,
- ✓ gromadzenie dokumentacji związanej z wykonywanymi audytami i kontrolami zgodnie z programem audytu lub kontroli z wykorzystaniem systemów informatycznych,
- ✓ gromadzenie danych, umożliwiających przygotowanie informacji na temat działalności komórki oraz przekazywanie ich właściwym jednostkom KAS,
- ✓ kontrola transakcji, o których mowa w tytule V rozdziale III rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 1306/2013 z dnia 17 grudnia 2013 r. w sprawie finansowania wspólnej polityki rolnej, zarządzania nią i monitorowania jej.

Szczegółowy zakres zadań określają regulaminy organizacyjne IAS w Gdańsku, obowiązujące w kontrolowanym okresie[2].

Zapoznanie się pracowników z aktami normatywnymi powszechnie obowiązującymi

W związku z tym, że kontrola obejmuje okres od 01.07.2024 r. do 31.12.2024 r. zweryfikowano, czy przed początkiem kontrolowanego okresu pracownicy ICE wykonali obowiązek zapoznania się z aktami normatywnymi powszechnie obowiązującymi z zakresu ochrony danych osobowych oraz bezpieczeństwa teleinformatycznego.

- ✓ Polityka Ochrony Danych Osobowych[3] - na podstawie raportu „Zestawienie zapoznania pracowników z dokumentem", wygenerowanego przez Naczelnika ICE z Qasystenta kontrolerzy ustalili, że 1 pracownik (M.J.[4]) zapoznał się po tym terminie, tj. 3.02.2025 r. Pracownicy, którzy rozpoczęli pracę w ICE w kontrolowanym okresie, zapoznali się bezzwłocznie, natomiast pozostali pracownicy – przed 1.07.2024 r.
  Obowiązek zapoznania się z dokumentem i potwierdzenia tego faktu w Qasystencie wynika z pisma DIAS w Gdańsku nr 2201-IWO-1.0140.1.2021 z 26.01.2021 r. Wyznaczony termin: 12.02.2021 r.

[redacted]

- ✓ Polityka Bezpieczeństwa Teleinformatycznego (wersja 2)[5] – na podstawie raportu Zestawienie zapoznania pracowników z dokumentem, wygenerowanego przez Naczelnika ICE z Qasystenta kontrolerzy ustalili, że tylko 1 pracownik zapoznał się z dokumentem po kontrolowanym okresie, tj. 3.02.2025 r. (J.B.[6])
  Obowiązek zapoznania się z dokumentem i potwierdzenia tego faktu w Qasystencie wynika z pisma DIAS w Gdańsku nr [redacted] r. Wyznaczony termin: 23.02.2024 r.

Pismem z 27.03.2025 r. Naczelnik ICE złożył wyjaśnienia w kwestii późniejszych dat zapoznania się pracowników z ww. aktami. Brak zapoznania się w terminie z Polityką Ochrony Danych Osobowych przez panią M.J. wynika z faktu, że pracownik rozpoczął pracę w ICE od 1.03.2024 r. (wcześniej świadczył pracę w US w Malborku), następnie od października 2024 r. do stycznia 2025 r. był na zwolnieniu lekarskim. Natomiast późniejsze zapoznanie się przez panią J.B z Polityką Bezpieczeństwa Teleinformatycznego (wersja 2) wynika z niedopatrzenia.

[Dowód: pismo–SZD, UNP: 2201-25-052024]

Uwagi kontrolerów

Wyjaśnienia Naczelnika nie zmieniają ustaleń kontroli. Zarówno Polityka Ochrony Danych Osobowych, jak i Polityka Bezpieczeństwa Teleinformatycznego są udostępnione w systemie Qasystent, w którym to systemie po zalogowaniu pojawia się komunikat o ilości i kategoriach dokumentów, z którymi pracownik nie zapoznał się. Poza tym w Qasystencie istnieje możliwość sporządzenia raportu „Zestawienie zapoznania się pracownika z dokumentacją" i w konsekwencji możliwość zweryfikowania, z jakimi dokumentami pracownik nie zapoznał się. Raport uwzględnia dokumenty wewnętrzne i zewnętrzne. Jest to narzędzie dostępne zarówno dla pracownika (w zakresie własnym), jak i dla kierownika (w odniesieniu do wszystkich podległych pracowników).
Reasumując, wskazane przez Naczelnika ICE okoliczności (w tym absencja pracownika od października 2024 r. do stycznia 2025 r.) nie usprawiedliwiają zapoznania się pracowników z wymaganą dokumentacją dopiero 3.02.2025 r. Zarówno pracownicy, jak i Naczelnik mieli możliwość zweryfikowania, czy obowiązek zapoznania się z dokumentami został zrealizowany.

Obowiązkowe szkolenia dla pracowników objętych badaniem

Dyrektor Izby Administracji Skarbowej w Gdańsku w pismach kierowanych m.in. do kierowników komórek organizacyjnych IAS w Gdańsku, polecił wszystkim pracownikom odbyć szkolenia z zakresu ochrony danych osobowych oraz bezpieczeństwa teleinformatycznego, wyznaczając terminy na ich realizację.

Przed początkiem okresu, którego dotyczy kontrola, tj. przed 1.07.2024 r., pracownicy byli zobowiązani do odbycia niżej wymienionych szkoleń. Kontrolerzy zweryfikowali, czy wszyscy

[redacted]

pracownicy ICE (według stanu na 31.12.2024 r.) odbyli szkolenia w terminie, przy czym na potrzeby kontroli przyjęto, że szkolenia odbyte w terminie, to szkolenia ukończone przed 1.07.2024 r.

- ✓ RODO Unijne rozporządzenie o ochronie danych osobowych – dostępne na platformie e-learningowej Atena 2, termin szkolenia: do 30.04.2018 r. Dla osób nowo zatrudnionych wyznaczono termin: przed przystąpieniem do realizacji obowiązków służbowych.
  26 pracowników odbyło szkolenia przed 1.07.2024 r., 1 pracownik odbył szkolenie dopiero 4.02.2025 r. (Ł.G.[7]). Pracownicy zatrudnieni 5.11.2024 r. odbyli szkolenia 8 i 12.11.2024 r. (A.K., A.M.[8]).
- ✓ Bezpieczeństwo teleinformatyczne w resorcie finansów – dostępne na platformie e-learningowej Atena 3, termin szkolenia: do 15.05.2024 r. Dla osób nowo zatrudnionych wyznaczono termin: przed przystąpieniem do realizacji obowiązków służbowych.
  Zobligowanych do odbycia szkolenia w wyznaczonym terminie było 26 pracowników.
  23 pracowników odbyło szkolenia przed 1.07.2024 r., 3 pracowników odbyło szkolenie po tej dacie (M.B. – 4.07.2024 r., E.M. – 1.08.2024 r., M.P. – 3.02.2025 r.)[9], pracownik zatrudniony 2.09.2024 r. – odbył szkolenie 9.09.2024 r., pracownicy zatrudnieni 5.11.2024 r. – w dniach 7 i 8.11.2024 r.
- ✓ Zasady bezpieczeństwa użytkowania systemów teleinformatycznych – dostępne na platformie e-learningowej moodle, termin szkolenia: do 21.06.2024 r.
  Zobligowanych do odbycia szkolenia w wyznaczonym terminie było 26 pracowników, 2 spośród nich odbyło szkolenia z opóźnieniem (M.B. – 3.07.2024 r., E.S. – 3.09.2024 r.)[10], pracownicy nowo zatrudnieni odbyli szkolenia dopiero 3 i 4.02.2025 r. (J.B., A.K., A.M.)[11,]
- ✓ Zasady bezpieczeństwa informacji – dostępne na platformie e-learningowej moodle, termin szkolenia: do 3.02.2023 r.
  Zobligowanych do odbycia szkolenia w wyznaczonym terminie było 26 pracowników.
  25 pracowników odbyło szkolenie przed 1.07.2024 r., 1 pracownik dopiero 3.02.2025 r. (M.P.[12]), pracownicy nowozatrudnieni odbyli szkolenia dopiero 3.02.2025 r. (.J.B, A.K., A.M.)[13]

Ponadto Dyrektor IAS w Gdańsku zobowiązał wszystkich pracowników i funkcjonariuszy do realizacji niżej wymienionych szkoleń:

[redacted]

- ✓ Bezpieczeństwo i ochrona ludności – dostępne na platformie e-learningowej Atena 3, wyznaczony termin szkolenia – do 30.09.2024 r. Dla osób nowo zatrudnionych wyznaczono termin: przed przystąpieniem do realizacji obowiązków służbowych. Zobligowanych do odbycia szkolenia w wyznaczonym terminie było 27 pracowników, 23 pracowników odbyło szkolenie w wyznaczonym terminie, 1 pracownik dopiero 11.02.2025 r. (M.G.[14]). 3 pracowników do dnia wszczęcia kontroli nie odbyło szkoleń (B.J., B.L., E.M.)[15], w tym nowy pracownik, zatrudniony 2.09.2024 r. Pracownicy zatrudnieni 5.11.2024 r. – odbyli szkolenia dopiero 13 i 15.11.2024 r.
- ✓ Przeciwdziałanie korupcji – dostępne na platformie e-learningowej Atena 3. Każdy nowo zatrudniony pracownik ma obowiązek zrealizować szkolenie w terminie 3 miesięcy od dnia rozpoczęcia pracy/pełnienia służby, pozostali pracownicy – cyklicznie, co 5 lat. W tym zakresie nie stwierdzono nieprawidłowości.

W piśmie z 27.03.2025 r. Naczelnik ICE wskazał przyczyny realizacji szkoleń po wyznaczonym terminie. Z wyjaśnień tych wynika, że:

- ✓ pani B.J. nie odbyła szkolenia z zakresu Bezpieczeństwo i ochrona ludności z uwagi na nieobecność w okresie od lipca 2024 r. do lutego 2025 r.,
- ✓ pani E.S. nie odbyła szkolenia z zakresu Zasady bezpieczeństwa użytkowania systemów teleinformatycznych z uwagi na nieobecność od 24.03.2024 r. do 2.09.2024 r.,
- ✓ pan Ł.G. odbył szkolenie z zakresu RODO Unijne rozporządzenie o ochronie danych osobowych dnia 02.03.2020 r. w ramach realizacji programu wprowadzania oraz szkolenie teoretyczne w służbie przygotowawczej,
- ✓ pani M.B. odbyła szkolenia z zakresu Bezpieczeństwo teleinformatyczne w resorcie finansów oraz Zasady bezpieczeństwa użytkowania systemów teleinformatycznych w dniach 3 i 4 lipca 2024 r., bezzwłocznie po zakończeniu długotrwałej nieobecności,
- ✓ pracownicy zatrudnieni 4.11.2024 r. realizowali szkolenia sukcesywnie. Szkolenia z zakresu RODO Unijne rozporządzenie o ochronie danych, Bezpieczeństwo teleinformatyczne w resorcie finansów, Bezpieczeństwo i ochrona ludności zostały zakończone przed przystąpieniem do realizacji obowiązków służbowych,
- ✓ nowozatrudnieni pracownicy odbyli szkolenia z zakresu Zasady bezpieczeństwa użytkowania systemów teleinformatycznych oraz Zasady bezpieczeństwa informacji dopiero 3.02.2025 r. ponieważ nie otrzymali informacji o konieczności odbycia tych szkoleń podczas spotkania dla nowozatrudnionych pracowników z IPP.

[Dowód: pismo–SZD, UNP: 2201-25-052024]

Powyższe wyjaśnienia uznano w całości.

Odnośnie pozostałych pracowników, którzy nie zrealizowali szkoleń w wyznaczonych terminach, Naczelnik ICE w piśmie z 27.03.2025 r. wyjaśnił, że:

[redacted]

- ✓ pani E.M. odbyła szkolenie z zakresu Bezpieczeństwo teleinformatyczne w resorcie finansów 1.08.2024 r. - w możliwie najszybszym dogodnym okresie z uwagi na realizację pilnych, terminowych zadań przydzielonych do realizacji oraz na urlop wypoczynkowy w miesiącach maj – sierpień 2024 r., natomiast z zakresu Bezpieczeństwo i ochrona ludności dopiero 7.03.2025 r. z uwagi na realizację pilnych i terminowych zadań.

Uwagi kontrolerów

Zweryfikowano, że pracownik przebywał na urlopie wypoczynkowym w dniach: 03.06.2024 r., 13.06.2024 r., 24.06.-02.07.2024 r., zatem miał możliwość wcześniej zrealizować szkolenia (przyp. terminów: 15.05.2024 r. i 30.09.2024 r.). Konieczność realizacji zleconych zadań nie może być usprawiedliwieniem dla niewykonania polecenia Dyrektora IAS, jakim jest odbycie szkolenia w wyznaczonym terminie.

- ✓ pani J.B. omyłkowo pominęła szkolenie z zakresu Bezpieczeństwo i ochrona ludności,
- ✓ pan M.G. nie odbył w terminie szkolenia z zakresu Bezpieczeństwo i ochrona ludności z uwagi na realizację pilnych i terminowych zadań wskazanych przez MF DAS w programach audytu.

Uwagi kontrolerów

Jak wcześniej wskazano, konieczność realizacji zleconych zadań nie może być usprawiedliwieniem dla niewykonania polecenia Dyrektora IAS, jakim jest odbycie szkolenia w wyznaczonym terminie.

- ✓ pani M.P. dopiero 3.02.2025 r. odbyła szkolenia z zakresu Bezpieczeństwo teleinformatyczne w resorcie finansów oraz Zasady bezpieczeństwa informacji ponieważ wcześniej nie miała informacji o obowiązku realizacji tych szkoleń. Z wyjaśnień pracownika wynika, że bezzwłocznie po otrzymaniu tej informacji zrealizował szkolenia.

Uwagi kontrolerów

Wyjaśnienia nie zmieniają ustaleń kontroli. Dyrektor IAS w Gdańsku pismami z 2.01.2023 r. oraz 15.05.2024 r.[16] polecił kierownikom komórek organizacyjnych zobligować wszystkich pracowników, w tym nowozatrudnionym do odbycia ww. szkoleń.

Brak realizacji szkoleń przez część pracowników, dowodzi, że nadzór w tym zakresie był niewystarczający. Pozytywnie jednak należy ocenić, że do dnia zakończenia kontroli wszyscy pracownicy ICE zrealizowali obowiązkowe szkolenia.

Uprawnienia do systemu informatycznego [redacted]

Z wyjaśnień Naczelnika ICE z 27.03.2025 r. wynika, że przegląd uprawnień dokonywany jest systematycznie podczas przeglądów centralnych/regionalnych. Naczelnik na bieżąco monitoruje zasadność i celowość utrzymywania uprawnień dostępowych, pracownikom

[redacted]

odchodzącym z komórki są odbierane uprawnienia, a pracownikom nowozatrudnionym są nadawane zgodnie ze zleconymi zadaniami, z uwzględnieniem okresu adaptacji nowego pracownika.

W tym zakresie nie stwierdzono nieprawidłowości.

Nadzór nad prawidłowością wykorzystywania danych z systemów informatycznych w ramach kontroli funkcjonalnej

Kwestie regulujące zasady sprawowania kontroli funkcjonalnej zostały określone w Instrukcji dot. szczegółowych zasad przeprowadzania kontroli funkcjonalnej sprawowanej w ramach nadzoru służbowego przez osoby zajmujące kierownicze stanowiska w Izbie Administracji Skarbowej w Gdańsku, urzędach skarbowych woj. pomorskiego i pomorskim urzędzie celno-skarbowym w Gdyni stanowiącą załącznik do zarządzenia Dyrektora Izby Administracji Skarbowej w Gdańsku[17].
Kontrola funkcjonalna powinna uwzględniać specyfikę zadań realizowanych przez daną komórkę organizacyjną i koncentrować się m.in. na organizacji i dyscyplinie służby i pracy, w tym przestrzeganiu przepisów o ochronie danych osobowych i Polityki Bezpieczeństwa Informacji Resortu Finansów.

Kontrola funkcjonalna sprawowana jest w oparciu o Plan Kontroli funkcjonalnej. Komórki organizacyjne zobowiązane są przesłać plan do komórki kontroli wewnętrznej Izby.
Na podstawie Planu kontroli funkcjonalnej na 2024 rok sporządzonego przez Naczelnika ICE ustalono, że zagadnienie z zakresu zasadności przetwarzania przez pracowników danych uzyskanych za pośrednictwem systemów informatycznych nie było przedmiotem kontroli.

W wyjaśnieniach z 27.03.2025 r. Naczelnik ICE wskazał, że w badanym okresie na bieżąco prowadził kontrolę funkcjonalną, która m.in. koncentrowała się na przestrzeganiu przez pracowników przepisów o ochronie danych osobowych i Polityki Bezpieczeństwa Informacji Resortu Finansów, w tym w zakresie „czystego biurka" i zamkniętych szaf, blokowania/wygaszania ekranu monitora. Ponadto na bieżąco podczas spotkań z pracownikami Wydziału ICE (Teams, spotkania bezpośrednie) zwracała szczególną uwagę na obowiązki pracowników m.in. w zakresie ochrony danych osobowych, przetwarzania danych i konsekwencjami nie przestrzegania zasad ochrony informacji oraz konieczności odbycia szkoleń w ww. zakresach.
Z uwagi na to, że w objętych kontrolą bieżącą przypadkach dot. zachowania przez pracowników zasad bezpieczeństwa informacji nie stwierdzono nieprawidłowości - nie podlegały one obowiązkowi dokumentowania w systemie [redacted](Kontrola funkcjonalna).
Ponadto Naczelnik ICE wskazał, że zgodnie z posiadanymi rolami i uprawnieniami do systemu informatycznego [redacted] nie posiada roli Raporty, co uniemożliwia weryfikację bezpośrednio działań pracowników w ww. systemie. Uprawnienia w zakresie generowania raportów z wejść

[redacted]

do systemu posiada, jako właściciel biznesowy aplikacji, Departament Kluczowych Podmiotów w MF. W ramach kontroli bieżącej zadań wykonywanych przez pracowników ICE weryfikowane są różne wątki, w tym te które wymagają sprawdzenia danych w systemie [redacted] Pracownicy przy pobieraniu danych z systemu podają powód pobrania danych/nr sprawy, w jakiej te dane są wykorzystywane. Pobrane dane, w minimalnym zakresie, w postaci zrzutów lub ściągniętych plików gromadzone są - co do zasady - w trakcie realizacji zadania na służbowym notebooku pracownika, do którego dostęp zabezpieczony jest poprzez logowanie domenowe.

[Dowód: pismo–SZD, UNP: 2201-25-052024]

Uwagi kontrolerów

Zgodnie z zasadami ww. zarządzenia Dyrektora IAS w Gdańsku, osoby zajmujące stanowiska kierownicze, winny uwzględnić w planach kontroli funkcjonalniej w szczególności ochronę danych osobowych. Formy nadzoru opisane w wyjaśnieniach są niewystarczające, z uwagi na stwierdzone, opisane w zagadnieniu drugim nieprawidłowości w zakresie naruszenia zasady ograniczenia celów przetwarzania danych osobowych. Należy stwierdzić, że organizacja pracy w ICE nie zapewnia w pełni rozliczalności działań w systemie [redacted]

Ustalenia

W działalności kontrolowanej komórki w przedstawionym powyżej zakresie stwierdzono następujące nieprawidłowości:

1. Znaczne przekroczenie terminu do zapoznania się z Polityką Ochrony Danych Osobowych przez 1 pracownika,
2. Znaczne przekroczenie terminu do zapoznania się z Polityką Bezpieczeństwa Teleinformatycznego (wersja 2) przez 1 pracownika,
3. Znaczne przekroczenie terminu do odbycia obowiązkowych szkoleń z zakresu: Bezpieczeństwo teleinformatyczne w resorcie finansów, Bezpieczeństwo i ochrona ludności, Zasady bezpieczeństwa informacji – w przypadku 4 pracowników,
4. Naczelnik ICE nie uwzględnił w planach kontroli funkcjonalnej w 2024 r. prawidłowości wykorzystania danych z systemów informatycznych, zagadnienie to nie było też objęte kontrolami doraźnymi.

Ocena cząstkowa:

Działalność komórki kontrolowanej należy ocenić pozytywnie z nieprawidłowościami.

III. 2 Zagadnienie drugie z zakresu badania: Wykorzystanie systemów informatycznych do celów służbowych.

Opis stanu faktycznego

Oceny dokonano w zakresie następujących zasad bezpieczeństwa informacji, określonych w Polityce Bezpieczeństwa Informacji Resortu Finansów, Polityce Ochrony Danych Osobowych Ministerstwa Finansów i Polityce Ochrony Danych Osobowych Izby Administracji Skarbowej w Gdańsku:

- ✓ dostępności – właściwość polegająca na zapewnieniu, że osoby upoważnione mają dostęp do informacji wtedy, gdy jest to potrzebne (różne zadania oznaczają różną wiedzę konieczną do ich wykonania, a tym samym, inny profil dostępu),
- ✓ poufności – właściwość polegająca na tym, że informacja nie jest udostępniana nieupoważnionym osobom, podmiotom lub procesom. Każda osoba posiada wiedzę o zasobie, do którego ma dostęp, ograniczoną wyłącznie do zagadnień, które są konieczne do realizacji powierzonych zadań służbowych,
- ✓ rozliczalności – właściwość zapewniająca, że działania osoby albo podmiotu mogą być przypisane w sposób jednoznaczny tylko tej osobie albo temu podmiotowi oraz pozwalająca umiejscowić ją w czasie,
- ✓ integralności – właściwość polegająca na zapewnieniu dokładności i kompletności informacji;

Zwrócono także uwagę na ograniczenie celów przetwarzania – cele przetwarzania danych osobowych muszą zostać jasno sprecyzowane, co pozwoli na spełnienie zasad rzetelności i przejrzystości (niezaprzeczalności) oraz dostępu osób do ich danych. Nie mogą one być dowolnie zmieniane i rozszerzane.

Realizacja zasady rozliczalności polega na zapewnieniu możliwości udokumentowania zgodności przetwarzania danych osobowych z zasadami określonymi w Polityce, bez względu na formę i sposób ich przetwarzania. Administrator jest odpowiedzialny za przestrzeganie ww. zasad oraz musi być w stanie wykazać ich przestrzeganie. Oznacza to, że w ramach uprawnień kontrolnych osób, których dane dotyczą, a także organu nadzorczego istnieje możliwość „rozliczenia" administratora oraz jego podwładnych.

Badanie oparto na informacjach przekazanych pismem z 26 lutego 2025 r. przez Departament Kluczowych Podmiotów.

Na cele kontroli udostępniono dane z [redacted] w zakresie danych podmiotów przeglądanych przez wytypowanych pracowników komórki ICE. Zbadano podstawę do wykorzystania w celach służbowych przedmiotowych danych z systemu [redacted]

System [redacted] to narzędzie informatyczne wspierające pracowników KAS realizujących procesy i zadania związane z obsługą Klientów zewnętrznych, służy przede wszystkim do skutecznej i sprawnej wizualizacji informacji z wielu różnych źródeł m. im. [redacted]

Narzędzie [redacted] stanowi miejsce szybkiej i sprawnej dostępności jak największej ilości informacji o danym podmiocie oraz o jego dotychczasowych i pożądanych działaniach wobec organów skarbowych.

Uprawnienia do systemy [redacted] nadawane są za pośrednictwem [redacted] Wniosek składa bezpośredni przełożony pracownika lub inna osoba posiadająca rolę kierowniczą w systemie [redacted] We wniosku wskazuje się role i uprawnienia do systemu [redacted] zgodnie z zakresem obowiązków pracownika.

Na podstawie zestawienia uprawnień i ról z systemu [redacted] przekazanego przez Naczelnika Wydziału ICE ustalono, że w kontrolowanym okresie do systemu [redacted] dostęp miało 24 pracowników (w tym Naczelnik Wydziału) z 29 zatrudnionych. Wszyscy posiadali rolę [redacted] ponadto Naczelnik wydziału posiadał rolę [redacted]

Do kontroli wytypowano 10 pracowników z 24 posiadających uprawnienia do systemu [redacted] Według list logowań do [redacted] przesłanej przez Ministerstwo Finansów, ustalono że z 10 wytypowanych pracowników 8 dokonywało przeglądu podmiotów w systemie i to ich objęto kontrolą. Dane przedstawia poniższa tabela.

Tabela nr 1

Lp.	Login AD	Imię i nazwisko	Łączna ilość sprawdzeń	Ilość przeglądanych podmiotów
1	[redacted]	J.B.2	109	31
2		M.C.	135	36
3		A.F.	275	83
4		Ł.G.	545	75
5		J.G.S.	brak	0
6		M.J.	45	8
7		N.K.	130	32
8		E.M.	brak	0
9		A.S.	3491	391
10		D.W.	190	24
		Razem	4920	680

Na podstawie raportów umożliwiających identyfikację użytkownika i sprawdzanego podmiotu oraz datę logowania i zakres przeglądanych danych przesłanych przez Ministerstwo Finansów, wytypowano 15 podmiotów, w stosunku do których przeglądany był największy zakres danych, celem ustalenia, czy przeglądanie miało związek z wykonywanymi czynnościami służbowymi.

Dane dotyczące wytypowanych podmiotów i złożonych wyjaśnień co do celu dokonanych odczytów w systemie przedstawia poniższa tabela.

Tabela nr 2

Lp.	Login AD pracownika	Data wyszukiwania / przeglądania podmiotu	Pesel/NIP podmiotu	Wyjaśnienia (w jakim celu dokonywano odczytu w systemie [redacted])
1	[redacted]	22.07.2024	[redacted]	Odczytu dokonano w ramach przeprowadzonego audytu. Pracownik nie pamięta powodu przeglądania danych

				podmiotu. Nie wyklucza „błędu ludzkiego”, polegającego na błędnym wprowadzeniu danych do systemu CRM-RF.
2	[redacted]	23.07.2024	[redacted]	Odczytu dokonano w ramach przeprowadzonego audytu. Weryfikacji podlegały powiązania członków komisji przetargowej z wykonawcami wybranymi do realizacji zamówienia.
3	[redacted]	25-26.07.2024	[redacted]	Odczytu dokonano w ramach przeprowadzonego audytu. Weryfikacji podlegało potwierdzenie bezstronności i braku konfliktu interesów eksperta oceniającego wniosek o dofinansowanie.
		22.08.2024	[redacted]	Odczytu dokonano w ramach przeprowadzonego audytu. Weryfikacji podlegało potwierdzenie braku powiązań i braku konfliktu interesów Beneficjenta z wykonawcą wybranym do realizacji zamówienia.
4	[redacted]	19.08.2024	[redacted]	Odczytu dokonano w ramach przeprowadzonego audytu. Weryfikacji podlegało potwierdzenie bezstronności i braku konfliktu interesów członka Komisji Oceny Projektów.
		19.08.2024	[redacted]	Odczytu dokonano w ramach przeprowadzonego audytu. Weryfikacji podlegało potwierdzenie braku powiązań pomiędzy wykonawcą a zamawiającym, w tym kierownika zamawiającego. Ponadto, weryfikacji podlegało potwierdzenie braku powiązań między kierownikiem jednostki zamawiającej a Członkami Komisji Oceny Projektów.
5	[redacted]	10.10.2024	[redacted]	Odczytu dokonano w ramach przeprowadzonego audytu. Weryfikacji podlegało potwierdzenie bezstronności i braku konfliktu interesów inspektora terenowego biorącego udział w kontroli projektu.
6	[redacted]	10.10.2024	[redacted]	Odczytu dokonano w ramach przeprowadzonego audytu. Weryfikacji podlegało potwierdzenie bezstronności i braku konfliktu interesów pracownika beneficjenta, który brał udział w procesie oceny wniosku o przyznanie pomocy.
7	[redacted]	14.11.2024	[redacted]	Odczytu dokonano w ramach przeprowadzonego audytu. Weryfikacji

				podlegało potwierdzenie braku konfliktu interesów pomiędzy zamawiającym a prezesem zarządu wykonawcy.
		15.11.2024	[redacted]	Odczytu dokonano w ramach przeprowadzonego audytu. Weryfikacji podlegało potwierdzenie braku konfliktu interesów pomiędzy zamawiającym a członkiem zarządu wykonawcy.
		14.11.2024	[redacted]	Odczytu dokonano w ramach przeprowadzonego audytu. Weryfikacji podlegało potwierdzenie braku konfliktu interesów członka komisji przetargowej.
		14.11.2024	[redacted]	Odczytu dokonano w ramach przeprowadzonego audytu. Weryfikacji podlegało potwierdzenie braku konfliktu interesów członka komisji przetargowej.
		14.11.2024	[redacted]	Odczytu dokonano w ramach przeprowadzonego audytu. Weryfikacji podlegało potwierdzenie braku konfliktu interesów pracownika beneficjenta.
		14.11.2024	[redacted]	Odczytu dokonano w ramach przeprowadzonego audytu. Weryfikacji podlegało potwierdzenie braku konfliktu interesów członka komisji przetargowej.
8	[redacted]	1,21,30 paź.2024	[redacted]	Odczytu dokonano w ramach kontroli transakcji ex-post. Pozyskanie niezbędnych informacji celem przedstawienia i opisania charakterystyki kontrolowanej jednostki.

W wyniku badania stwierdzono, że w 14 przypadkach (poz. od 2 do 8 w tabeli nr 2) przeglądanie danych miało związek z wykonywaniem czynności służbowych przez pracowników, co zostało potwierdzone odpowiednimi dokumentami przez Naczelnika Wydziału.

[Dowód: pismo –SZD, UNP: .2201-25-052953]

Kontrolerzy ustalili, że w 1 przypadku (poz. 1 w tabeli nr 2) przeglądanie danych nie było związane z wykonywanymi czynnościami służbowymi, co stanowi nieprawidłowość. Nieuprawniony dostęp do danych podmiotu w [redacted] stanowi incydent bezpieczeństwa informacji.

Naczelnik Wydziału wyjaśnił, że pracownik po przeanalizowaniu dokumentacji z audytu, wskazał, że nie posiada raportów ani zrzutów z ekranu dla przeglądanego podmiotu. Zakres przeprowadzonego audytu był obszerny, badaniu podlegał konflikt interesów z tytułu zamówień publicznych, statusu ostatecznych odbiorców pomocy oraz kontrahenci powiązani z beneficjentami pomocy. Z uwagi na tak odległy czas (8 miesięcy od zdarzenia) pracownik nie

pamięta powodu przeglądania danych podmiotu. Nie wyklucza „błędu ludzkiego", polegającego na błędnym wprowadzeniu danych do systemu [redacted] w celu przeglądania danych tego podmiotu. W dalszej części wyjaśnień wskazuje, że w momencie zauważenia pomyłki, pracownik zaprzestał przeglądania danych, nie pobierając żadnych dowodów dotyczących wejścia do systemu w odniesieniu do wskazanego podmiotu. Naczelnik poinformował, że po ponownej weryfikacji dokumentacji zgromadzonej na komputerze pracownika, ustalono, że nie posiada on żadnych plików zapisanych z danymi podmiotu. Pracownik wyjaśnił również, że w wyniku przeprowadzonej weryfikacji dokumentacji zgromadzonej w trakcie przeprowadzonego audytu, w terminie przeglądu danych podmiotu zostały wyświetlone pliki, w których wykazano obecność takiego samego nazwiska jak nazwisko podmiotu przeglądanego. W załączeniu przekazano nw. pliki :

- sprzedaz_[redacted]
- sprzedaz_[redacted]

Naczelnik wskazał, że powyższy fakt potwierdza, że dane podmiotu zostały omyłkowo przez pracownika wprowadzone w systemie [redacted] Pracownik oświadczył Naczelnikowi, że informacje te nie zostały przez niego dalej przekazane w celach służbowych czy prywatnych.
W dalszej części Naczelnik wskazał, że z uwagi na fakt, że nie doszło do pobrania i eksportowania danych nie wystąpił incydent w przetwarzaniu danych osobowych, który prowadziłby do naruszenia bezpieczeństwa danych skutkujących przypadkowym lub niezgodnym z prawem zniszczeniem, utratą, modyfikacją, nieuprawnionym ujawnieniem lub dostępem do danych osobowych. Ponadto pracownik oświadczył Naczelnikowi, że wyżej wymieniona osoba nie jest mu znana zarówno w sferze prywatnej jak i służbowej. W związku z powyższym nie nastąpiło żadne naruszenie praw tej osoby. Dlatego też pracownik uznał, że wyżej wymieniona sytuacja nie wymaga dalszego procedowania.

Zdaniem Naczelnika, w powyższej sytuacji przeglądanie danych związanych z realizacją zadań służbowych nie wpłynęło na naruszenie zasady rozliczalności, gdyż dane te nie zostały w żaden sposób przetworzone, tj. pobrane, utrwalone czy wykorzystane.

Jednocześnie podkreślił, że system kontroli treści [redacted] weryfikuje dane w celu zapobiegania wyciekowi danych wrażliwych, w co wyposażony jest każdy komputer służbowy pracownika ICE.

Naczelnik wskazał, że w IAS w Gdańsku nie został do dnia dzisiejszego powołany koordynator lokalny czy konsultant systemu [redacted] który mógłby ewentualnie określić zasady korzystania z ww. systemu.

[Dowód: pismo –SZD, UNP: 2201-25-059324]

Uwagi kontrolerów

Trudno uznać, że sprawdzenie wynikało z błędu ludzkiego, ponieważ 22.07.2024 r. pracownik dokonał w systemie [redacted] odczytu danych tylko jednego podmiotu. Ponadto pracownik w kontrolowanym okresie tj. 01.07.2024 r. – 31.12.2024 r. nie dokonywał odczytu danych osób o tym samym nazwisku, wskazanych w przesłanych do wyjaśnień plikach. W kwestii

zaprzestania przeglądania danych, nie można uznać wyjaśnień z uwagi na szeroki zakres przeglądanych danych z teczki [redacted] oraz duży zakres czasu dostępu do danych od 9:50 do 10:11. Fakt nie posiadania przez pracownika na komputerze służbowym zapisanych plików z danymi podmiotu, nie przesądza o niewystąpieniu incydentu bezpieczeństwa danych. Zgodnie z Polityką Zarządzania Incydentami Bezpieczeństwa Informacji w Resorcie Finansów świadome lub przypadkowe naruszenie zasad bezpieczeństwa informacji poprzez nieuprawniony dostęp do danych osobowych stanowi incydent bezpieczeństwa.

Ponadto, brak możliwości udokumentowania związku przeglądanych danych z realizowanymi zadaniami służbowymi zgodnie z Polityką Ochrony Danych Osobowych Izby Administracji Skarbowej w Gdańsku, wbrew stanowisku Naczelnika Wydziału narusza zasadę rozliczalności poprzez przetwarzanie niezgodnie z zasadą ograniczenia celów przetwarzania danych osobowych.

System [redacted] w który wyposażone są komputery służbowe pracowników ICE, nie jest narzędziem ochrony przed nieuprawnionym przeglądaniem danych w systemach centralnych, w tym [redacted] System ten wykorzystywany jest do monitorowania i ochrony informacji elektronicznej, a w przedmiotowej sprawie zgodnie z wyjaśnieniami Naczelnika dane przeglądanego podmiotu nie zostały pobrane czy utrwalane na komputerze służbowym pracownika.

Zasady korzystania z systemów teleinformatycznych uregulowane są m.in. w Polityce Ochrony Danych Osobowych Izby Administracji Skarbowej w Gdańsku, Polityce Ochrony Danych Osobowych Ministerstwa Finansów, Polityce Bezpieczeństwa Teleinformatycznego Resortu Finansów, Polityce Bezpieczeństwa Informacji Resortu Finansów, kwestia braku koordynatora lokalnego czy konsultanta systemu [redacted] w IAS w Gdańsku, nie wpływa na ustalenia kontrolerów. Wsparciem użytkowników systemu [redacted] zajmuje się Centrum Kompetencyjne Obsługi Systemu Zarządzania Relacjami z Klientami Resortu Finansów w Zielonej Górze.

Ustalenia

W działalności kontrolowanej komórki w przedstawionym powyżej zakresie stwierdzono w jednym przypadku nieprawidłowość, polegającą na naruszeniu zasady rozliczalności – przeglądaniu danych podmiotu wobec którego pracownik nie wykonywał zadań służbowych, co stanowi incydent bezpieczeństwa informacji. Zgodnie z Polityką Bezpieczeństwa Informacji Resortu Finansów, naruszenie bezpieczeństwa informacji może być uznane za ciężkie naruszenie obowiązków pracowniczych, a w konsekwencji może powodować odpowiedzialność dyscyplinarną.

Ocena cząstkowa:

Działalność komórki kontrolowanej w zakresie wykorzystania systemów informatycznych do celów służbowych należy ocenić **negatywnie.**

IV. Pozostałe informacje

Przedstawiając powyższe polecam:

1. terminowo zapoznawać się z aktami normatywnymi powszechnie obowiązującymi oraz realizować obowiązkowe szkolenia,
2. zwiększyć nadzór nad realizacją zadań wymienionych w pkt 1,
3. przestrzegać zasad bezpieczeństwa dotyczących eksploatacji systemów teleinformatycznych, określonych w Polityce Bezpieczeństwa Informacji Resortu Finansów, Polityce Ochrony Danych Osobowych Ministerstwa Finansów i Polityce Ochrony Danych Osobowych Izby Administracji Skarbowej w Gdańsku,
4. przeprowadzać cyklicznie kontrolę funkcjonalną w temacie prawidłowość wykorzystywania przez pracowników danych z systemów informatycznych, uwzględnić ten temat w planach kontroli funkcjonalnej,

Zgodnie z § 33 ust. 6 instrukcji w sprawie szczegółowych zasad przeprowadzania kontroli wewnętrznej w komórkach organizacyjnych Izby Administracji Skarbowej w Gdańsku od wystąpienia pokontrolnego nie przysługują środki odwoławcze.

Na podstawie § 41 instrukcji w sprawie szczegółowych zasad przeprowadzania kontroli wewnętrznej w komórkach organizacyjnych Izby Administracji Skarbowej w Gdańsku, w związku z przedstawionymi powyżej ustaleniami kontroli, proszę o przedłożenie w terminie 1 miesiąca od daty otrzymania niniejszego wystąpienia pokontrolnego informacji o sposobie wykorzystania zaleceń, wykorzystania wniosków lub przyczynach ich niewykorzystania albo o innym sposobie usunięcia stwierdzonych nieprawidłowości.

Jednocześnie w związku z poleceniem Ministerstwa Finansów zobowiązuję do przekazania do dyrektora informacji o rezultatach wdrożonych zaleceń pokontrolnych w terminie 9 miesięcy licząc od daty sporządzenia przez komórkę kontrolowaną informacji o zrealizowaniu zaleceń pokontrolnych. Informacje w powyższym zakresie powinny wskazywać konkretne działania i sposób ich realizacji.

Wystąpienie pokontrolne zostało sporządzone w formie elektronicznej, przesłane do kierownika komórki kontrolowanej za pośrednictwem SZD.

Gdańsk, 18 czerwca 2025 roku

Z wyrazami szacunku

Dyrektor
Izby Administracji Skarbowej
w Gdańsku

Czesław Kalinowski
(kwalifikowany podpis elektroniczny)