DYREKTOR
IZBY ADMINISTRACJI SKARBOWEJ
W POZNANIU

Poznań, 30 grudnia 2025 roku

UNP: 3001-25-242309

Znak sprawy: **3001-IWW1.0921.18.2025**

Pani

Barbara Jaś
Naczelnik
Urzędu Skarbowego w Ostrowie
Wielkopolskim
ul. Chłapowskiego 45
63-400 Ostrów Wielkopolski

WYSTĄPIENIE POKONTROLNE	
Sporządzone na podstawie art. 46 i art. 47 ustawy z dnia 15 lipca 2011 r. o kontroli w administracji rządowej (t.j. Dz. U. z 2020, poz. 224 ze zm.) w brzmieniu obowiązującym przed 6 września 2025 r.	
Nazwa i adres kontrolowanego urzędu	
3017 Urząd Skarbowy w Ostrowie Wielkopolskim **ul. Chłapowskiego 45,** **63-400 Ostrów Wielkopolski**	
Naczelnik kontrolowanego urzędu	
Pan Krzysztof Chmielewski (do 30 listopada 2023 r.), Pani Gabriela Grygiel (od 1 grudnia 2023 r. do 21 maja 2024 r.), Pani Barbara Jaś (od 22 maja 2024 r.).	
Upoważnienie do przeprowadzenia kontroli	
Nr 22/2025 z 9 lipca 2025 r. i nr 31/2025 z 1 października 2025 r. wydane przez Dyrektora Izby Administracji Skarbowej w Poznaniu.	
Wpis do książki kontroli	
Kontrola w trybie zwykłym wpisana pod pozycją nr 2/2025.	
Koordynator kontroli – imię, nazwisko i stanowisko służbowe/stopień służbowy	
Karolina Stróżczyk główny ekspert skarbowy	
Kontrolerzy – imię, nazwisko i stanowisko służbowe/stopień służbowy	
1.	Anna Pacholska – ekspert skarbowy
2.	Karolina Stróżczyk – główny ekspert skarbowy

Data rozpoczęcia czynności kontrolnych	21 lipca 2025 r.
Data zakończenia czynności kontrolnych	8 grudnia 2025 r.
Zakres kontroli	
Przedmiot kontroli	Prawidłowość wykorzystania systemów informatycznych.
Okres objęty kontrolą	Od 1 stycznia 2019 r. do 31 grudnia 2024 r. Badaniem mogły zostać objęte również zdarzenia i dokumenty wcześniejsze lub późniejsze, gdy miały związek z przedmiotem kontroli.
Kontrolowany obszar działalności	
Bezpieczeństwo i ochrona informacji.	
Cel kontroli	
Ocena, czy pracownicy Urzędu Skarbowego w Ostrowie Wielkopolskim wykorzystywali informacje (w tym dane osobowe) z systemów informatycznych wyłącznie do realizacji zadań służbowych, a także czy Naczelnik Urzędu wdrożył mechanizmy zapobiegające nieuprawnionemu wykorzystaniu danych z systemów informatycznych.	
Ocena skontrolowanej działalności	
Negatywna.	
DOKONANE USTALENIA FAKTYCZNE	

I. Organizacja pracy urzędu w zakresie korzystania z systemów informatycznych

W Urzędzie Skarbowym w Ostrowie Wielkopolskim strukturę organizacyjną, zakres zadań komórek organizacyjnych, zasady organizacji pracy, zakres nadzoru sprawowanego przez Naczelnika Urzędu Skarbowego i Zastępców, zakres stałych uprawnień i zakres upoważnień określały:

- Regulamin Organizacyjny stanowiący Załącznik nr 16 do Zarządzenia Dyrektora Izby Administracji Skarbowej w Poznaniu nr 15/2017[1] z dnia 9 marca 2017 r. (obowiązujący do 11 listopada 2019 r.),
- Zarządzenie Nr 127/2019[2] Dyrektora Izby Administracji Skarbowej w Poznaniu z dnia 24 października 2019 r. w sprawie nadania Regulaminu Organizacyjnego Urzędowi Skarbowemu w Ostrowie Wielkopolskim (obowiązujące od 12 listopada 2019 r. do 31 sierpnia 2021 r.),
- Zarządzenie Nr 137/2021[3] Dyrektora Izby Administracji Skarbowej w Poznaniu z dnia 12 sierpnia 2021 r. w sprawie nadania Regulaminu Organizacyjnego Urzędowi Skarbowemu w Ostrowie Wielkopolskim (obowiązujące od 1 września 2021 r. do 31 października 2022 r.),
- Zarządzenie Nr 182/2022 Dyrektora Izby Administracji Skarbowej w Poznaniu z dnia 25 października 2022 r. w sprawie nadania Regulaminu Organizacyjnego Urzędowi Skarbowemu w Ostrowie Wielkopolskim (obowiązujące od dnia 1 listopada 2022 r. do 31 grudnia 2022 r.),
- Zarządzenie Nr 241/2022 Dyrektora Izby Administracji Skarbowej w Poznaniu z dnia 22 grudnia

[1] Zmienionego Zarządzeniem Nr 24/2018 Dyrektora Izby Administracji Skarbowej w Poznaniu z dnia 27 lutego 2018 r.

[2] Zmienione Zarządzeniem Nr 91/2020 Dyrektora Izby Administracji Skarbowej w Poznaniu z dnia 19 sierpnia 2020 r. zmieniającym Regulamin Organizacyjny Urzędu Skarbowego w Ostrowie Wlkp.

[3] Zmienione Zarządzeniem Nr 45/2021 Dyrektora Izby Administracji Skarbowej w Poznaniu z dnia 15 marca 2021 r. zmieniającym Regulamin Organizacyjny Urzędu Skarbowego w Ostrowie Wielkopolskim oraz Zarządzeniem Nr 26/2022 Dyrektora Izby Administracji Skarbowej w Poznaniu z dnia 24 lutego 2022 r. zmieniające Regulamin Organizacyjny Urzędu Skarbowego w Ostrowie Wielkopolskim

2022 r. w sprawie nadania Regulaminu Organizacyjnego Urzędowi Skarbowemu w Ostrowie Wielkopolskim (obowiązujące od 1 stycznia 2023 r. do 16 maja 2025 r.).

Nadzór nad realizacją zadań sprawowali:

1. Naczelnicy Urzędu – pan Krzysztof Chmielewski (do 30 listopada 2023 r.), pani Gabriela Grygiel (od 1 grudnia 2023 r. do 21 maja 2024 r.), pani Barbara Jaś (od 22 maja 2024 r.),
2. Zastępcy Naczelnika:

   ZN1: pani Arleta Leki (od 8 marca 2017 r. do 28 lutego 2022 r.), pan Rafał Nawrot (od 1 listopada 2022 r. do 5 sierpnia 2024 r.), pan Jacek Syrkiewicz (od 6 sierpnia 2024 r. do nadal); w okresie od 1 marca 2022 r. do 30 października 2022 r. nie było osoby powołanej na zastępcę naczelnika ZN1.
   ZN2: pani Justyna Mularczyk (od 9 marca 2020 r. do 16 stycznia 2022 r.), pan Marcin Kużaj ZN2 (od 15 kwietnia 2022 r. do 5 sierpnia 2024 r.), pani Małgorzata Klońska ZN2 (od 6 sierpnia 2024 r. do nadal); w okresach od 1 stycznia 2019 r. do 8 marca 2020 r. i od 17 stycznia 2022 r. do 14 kwietnia 2022 r. nie było osoby powołanej na zastępcę naczelnika ZN2.

Z Regulaminów Organizacyjnych wynika, że do zadań wszystkich komórek należy wykonywanie zadań w sposób zgodny z prawem, efektywny, oszczędny i terminowy oraz przestrzeganie zasad bezpiecznego przetwarzania informacji.
Zastępca NUS w zakresie powierzonych spraw czuwa nad przestrzeganiem dyscypliny pracy oraz tajemnicy państwowej, służbowej, skarbowej (…).
Kierownicy komórek przestrzegają obowiązujących przepisów w zakresie tajemnicy służbowej, skarbowej, ochrony danych osobowych, bezpieczeństwa i higieny pracy, a także nadzorują w tym zakresie pracowników.

Kontrolą objęto pracowników zatrudnionych na dzień 31 grudnia 2024 r. w:

- 2 komórkach w Pionie Kontroli tj. komórce kontroli podatkowej (SKP) oraz komórce czynności sprawdzających i analiz (SKA-2),
- komórce w Pionie Orzecznictwa tj. komórce postępowań podatkowych (SPO),
- 4 zastępców NUS (Małgorzata Klońska, Marcin Kużaj, Rafał Nawrot, Jacek Syrkiewicz),

łącznie 19 osób.
Na przestrzeni kontrolowanego okresu wielokrotnie zmieniała się struktura organizacyjna kontrolowanej jednostki. W zakresie badanych komórek:
Pion Orzecznictwa – w kontrolowanym okresie podlegał bezpośrednio NUS. Do 11 listopada 2019 r. w Pionie funkcjonowały dwie komórki:

- Dział Podatków Dochodowych i Podatku od Towarów i Usług (SPV),
- Wieloosobowe Stanowisko Podatków Majątkowych i Sektorowych (SPM).

Następnie w związku z wejściem w życie Regulaminu Organizacyjnego wprowadzonego Zarządzeniem DIAS w Poznaniu nr 127/2019 utworzono Dział Podatków Dochodowych i Podatku od Towarów i Usług oraz Podatków Majątkowych i Sektorowych (SPV), który funkcjonował do 31 sierpnia 2021 r.
Od 1 września 2021 r. utworzono Dział Postępowania Podatkowego (SPO).
Pion Kontroli w kontrolowanym okresie podlegał Drugiemu Zastępcy NUS (ZN2). W całym kontrolowanym okresie funkcjonował Dział Kontroli Podatkowej (SKP).

Drugi Referat Czynności Analitycznych i Sprawdzających został przekształcony od 12 listopada 2019 r. w Drugi Dział Czynności Analitycznych i Sprawdzających (SKA-2).

Koordynator do spraw ochrony danych osobowych

Funkcję koordynatora do spraw ochrony danych osobowych pełnią osoby wchodzące w skład Zespołu Inspektora Ochrony danych w IAS w Poznaniu (Decyzja Dyrektora IAS w Poznaniu nr 31/2024 z 13 czerwca 2024 roku) – (…) i (…)[4].

Obowiązkowe szkolenia

Szkolenia okresowe z zakresu ochrony informacji prawnie chronionych zgodnie z § 25.5 Polityki Bezpieczeństwa Informacji w Izbie Administracji Skarbowej w Poznaniu odbywają się również w formie e-learningowej. Wszyscy pracownicy/funkcjonariusze mający dostęp do systemów informatycznych byli zobowiązani do ukończenia szkoleń e-learningowych na platformie Atena3 (wcześniej Atena2).
Pracownicy mieli obowiązek ukończyć szkolenia z zakresu:

- RODO Unijne rozporządzenie o ochronie danych osobowych,
- Bezpieczeństwo informacji w Resorcie Finansów (Atena 3),
- Bezpieczeństwo teleinformatyczne – szkolenie dedykowane dla pracowników resortu finansów, dostępne na platformie e-learningowej Atena2,
- Bezpieczeństwo teleinformatyczne w resorcie finansów (Atena3).

Wg danych z platformy e-learningowej Atena3 (wcześniej Atena2) udostępnionych przez Wydział Personalny (IPP) tut. IAS ustalono, że:

1. Szkolenia RODO Unijne rozporządzenie o ochronie danych osobowych nie ukończyła (…). Pozostali pracownicy ukończyli szkolenie w 2018 r. lub w przypadku zatrudnienia po tym roku niezwłocznie po zatrudnieniu
   NUS 24 września 2025 r. wyjaśnił, że (…) nie ukończyła szkolenia ze względu na długotrwałą nieobecność. Wyjaśnienie nie zmienia ustaleń kontroli. Szkolenie powinno zostać ukończone po powrocie do pracy.

2. Zgodnie z pismem Departamentu Bezpieczeństwa i Ochrony Informacji DB1.0125.22 z 31 marca 2022 r. wszyscy pracownicy zostali zobowiązani do ponownego ukończenia do 30 czerwca 2022 r. szkolenia „Bezpieczeństwo teleinformatyczne – szkolenie dedykowane dla pracowników resortu finansów" (poprzednie szkolenia odbyły się w 2016 roku). Termin ten został następnie przesunięty na 31 sierpnia 2022 r. Ustalono, że:
   - szkolenia przypominającego nie ukończyli: (…), (…), (…), (…); NUS w wyjaśnieniu jako przyczyny nieukończenia szkolenia wskazywał na dłuższe nieobecności oraz przeoczenie,
   - z opóźnieniem szkolenie ukończyła (…) (29 września 2022 r.), NUS jako przyczynę podał przeoczenie i wykonywanie innych czynności służbowych,
   - zatrudniona z dniem 4 lipca 2022 r. (…) szkolenie odbyła 7 lipca 2022 r., tj. niezwłocznie po zatrudnieniu,
   - pozostałych 12 pracowników ukończyło szkolenie przypominające w terminie do 30 czerwca 2022 r.

3. Szkolenie „Bezpieczeństwo teleinformatyczne w resorcie finansów" (Atena3) należało ukończyć do 15 maja 2024 r. W kontrolowanej jednostce pracownicy ukończyli szkolenie w wymaganym

[4] Podobnie jak w poprzednich latach – decyzje DIAS w Poznaniu nr 13/2020, 21/2022 oraz 28/2019.

terminie lub po powrocie z dłuższej nieobecności.

4. Szkolenie „Bezpieczeństwo informacji w Resorcie Finansów” (Atena3) należało ukończyć do 15 listopada 2024 r. W badanej próbie 19 pracowników:

- w 2 przypadkach pracownicy ukończyli szkolenie 9 grudnia 2024 r. (po dłuższej nieobecności, w innym US, do którego zostali przeniesieni),
- 15 pracowników ukończyło szkolenie w wymaganym terminie,
- 2 pracowników ukończyło szkolenie 18 lipca 2025 r., po powrocie z dłuższej nieobecności (i po otrzymaniu informacji przypominającej o konieczności odbycia szkolenia).

Podsumowując, stwierdzono przypadki nieukończenia obowiązkowych szkoleń (Szkolenia RODO Unijne rozporządzenie o ochronie danych osobowych – 1 pracownik, szkolenie „Bezpieczeństwo teleinformatyczne – szkolenie dedykowane dla pracowników resortu finansów” – 4 pracowników), co stanowi nieprawidłowość**.** Osoby odpowiedzialne – pracownicy: (…), (…), (…), (…) oraz w trybie nadzoru kierownicy komórek. W zakresie ww. pracowników stwierdzono w toku kontroli, przypadki przeglądania danych bez związku z prowadzoną sprawą. Niewłaściwe działanie ze strony pracowników mogło wynikać m.in. z braku właściwego przeszkolenia i skutkowało naruszeniem przepisów prawa.

W toku kontroli stwierdzono również ukończenie przez pracowników szkoleń z opóźnieniem, co stanowi uchybienie.

Zapoznanie pracowników z Polityką Ochrony Danych Osobowych

W związku z wejściem w życie w 2021 r. Zarządzenia Ministra Finansów, Funduszy i Polityki Regionalnej z dnia 29 grudnia 2020 r. w sprawie wprowadzenia Polityki Ochrony Danych Osobowych, pracownicy zobowiązani zostali do zapoznania się z zasadami określonymi w wyżej wymienionej Polityce.

W badanej próbie kontrolnej pracownicy potwierdzili zapoznanie się z Polityką Ochrony Danych Osobowych wprowadzoną Zarządzeniem Ministra Finansów, Funduszy i Polityki Regionalnej z dnia 29 grudnia 2020 r.

Oświadczenia po odbytym szkoleniu z zakresu informacji prawnie chronionych zbierane są od osób nowo zatrudnionych oraz osób, które odbywają szkolenia przypominające z informacji prawnie chronionych.

Upoważnienie do przetwarzania danych osobowych

Wszyscy kontrolowani pracownicy (19 osób) posiadali w kontrolowanym okresie aktualne upoważnienia do przetwarzania danych osobowych i podpisali stosowne oświadczenie dot. ochrony danych osobowych[5].

Sprawozdanie z przeglądu ochrony danych osobowych

Pracownik komórki Wieloosobowego Stanowiska Ochrony Danych (IWD) tutejszej IAS, na podstawie upoważnienia nr 3001-IWD.0140.96.2025 r., w dniu 27 maja 2025 r. przeprowadził kontrolę w zakresie przestrzegania przepisów o ochronie danych osobowych w Urzędzie Skarbowym w Ostrowie Wielkopolskim. Przeglądem objęto okres od 21 sierpnia 2019 r. do 27 maja 2025 r.

Z przeprowadzonego przeglądu sporządzono sprawozdanie datowane na 16 lipca 2025 r.

[5]Informacje uzyskane z komórki IWD tut. IAS UNP 3001-25-141523.

Uprawnienia do systemów informatycznych

Badanie przeprowadzono na podstawie raportu 10 – Raport o uprawnieniach i rolach użytkownika z Centralnego Systemu Zarządzania Uprawnieniami i Uwierzytelniania Użytkowników (CSU) oraz raportów z Qasystent „Uprawnienia użytkownika w aplikacjach w określonym przedziale czasowym". Informacje uzupełniono w toku kontroli o wyjaśnienia NUS. Zbadano uprawnienia nadane 19 pracownikom Urzędu Skarbowego w Ostrowie Wielkopolskim.

Aktualnie uprawnienia do systemu informatycznego PoltaxPlus w Urzędzie Skarbowym w Ostrowie Wielkopolskim nadawane są z wykorzystaniem CSU – Centralnego Systemu Zarządzania Uprawnieniami i Uwierzytelniania Użytkowników. W zakresie pozostałych uprawnień do realizacji procesu zarządzania uprawnieniami do systemów informatycznych wykorzystywany jest system Qasystent[6].

W 2022 r. nastąpiła zmiana sposobu nadawania uprawnień w systemie PoltaxPlus. Do maja 2022 r. nadawanie uprawnień realizowane było z wykorzystaniem uprawnień o charakterze jednostkowym (tzw. atomowym). Od czerwca 2022 r. nadawanie uprawnień dokonywane jest w oparciu o koncepcję tzw. ról stanowiskowych (RS).

W kontrolowanym okresie kierownik i pracownicy komórek SKA-2, SPO, SKP oraz Zastępcy NUS posiadali dostęp do systemu PoltaxPlus US w Ostrowie Wielkopolskim (a także w ramach uprawnień nadawanych przez CSU do Podatnik360). Pracownicy posiadali także dostępy do innych systemów wykorzystywanych w pracy m.in. WRO-SYSTEM, SZD - System Zarządzania Dokumentami, SSP – Scentralizowany System Poboru, EUREKA – System Informacji Celno-Skarbowej, WIS – Wiążąca Informacja Stawkowa, BPS - Baza Podmiotów Szczególnych[7], ZISAR PLUS, KARTA 2 i innych.

Badanie przeprowadzono według stanu na 31 grudnia 2024 r. Zasadniczo nadane uprawnienia odpowiadały zakresowi czynności realizowanemu przez pracowników. Zastępcy NUS odpowiedzialni za Pion Poboru i Egzekucji nie posiadali uprawnień do modułu WIERZYTELNOŚCI we WRO-System, co mogło utrudniać sprawowanie nadzoru w zakresie egzekucji administracyjnej. Ponadto zgodnie z zaleceniami MF wszyscy pracownicy powinni mieć nadany dostęp do systemu EUREKA – dotyczy to również zastępców NUS. W badanej próbie ZNUS odpowiedzialny za Pion Poboru i Egzekucji takich uprawnień nie posiadał. NUS w toku kontroli wystąpił o nadanie uprawnień do WRO-System i systemu EUREKA Zastępcy NUS.

W zakresie systemu Zefir2 pracownik ma nadane uprawnienia do rejestrowania i stornowania dokumentu (AK.RW.001 i AK.RW.003). Analiza wskazuje, że uprawnienia te nie są adekwatne do realizowanych zadań w komórce SKP. Wg administratora systemu ZEFIR 2 w tut. IAS w komórce kontroli podatkowej najwłaściwszymi są uprawnienia AK.RO.001, AK.WP.001 i AK.WP.010.

Aktualnie poza uprawnieniami AK.RW.001 i AK.RW.003 pozostałe nadane uprawnienia umożliwiają jedynie przeglądanie danych – należałoby jednak dokonać ponownej analizy pod kątem racjonalności ich posiadania przez pracownika SKP. Pobrano w tym zakresie wyjaśnienia do kontrolowanej jednostki.

[6] Zarządzenie Nr 127/2018 Dyrektora Izby Administracji Skarbowej w Poznaniu z dnia 28 września 2018 r. w sprawie wykorzystania systemu Qasystent do realizacji procesu zarządzania uprawnieniami do systemów informatycznych funkcjonujących w Izbie Administracji Skarbowej w Poznaniu i podległych urzędach, zmienione Zarządzeniem Nr 58/2019 Dyrektora Izby Administracji Skarbowej w Poznaniu z dnia 27 maja 2019 r.

[7] Baza Podmiotów Szczególnych została wycofana z eksploatacji z końcem września 2024 r.

Według NUS nadane uprawnienia wykorzystywane są do realizacji zadania z uwagi na prowadzenie postępowań podatkowych w komórce SKP.

Odnosząc się do tego wyjaśnienia, ostateczną decyzję o jakie uprawnienia dla pracownika należy zawnioskować podejmuje NUS i w związku z tym jest on odpowiedzialny za właściwe wykorzystanie systemu informatycznego.

Wg danych z Qasystent'a poszczególni pracownicy posiadają dostępy do systemu lokalnego [3017] Ewidencje GUI. Faktycznie jest to system o nazwie Ewidencje US i przełożony pracownika powinien zgłosić w Qasystencie wniosek o nadanie, modyfikację lub odebranie uprawnień w odpowiednim systemie wewnętrznym [30XX] Ewidencje US.

Wg wyjaśnienia NUS z 18 września 2025 r. wystąpiono w CSD o dokonanie aktualizacji nazwy: system wewnętrzny [3017] Ewidencje US. Pozytywnie oceniono podjęcie działań w celu zmiany nazwy systemu lokalnego w Qasystent.

Uwzględniono wyjaśnienia kontrolowanej jednostki odnośnie do nienadania uprawnień do JPK_Lunetka 2 pracownikom komórki postępowań podatkowych. Byli to pracownicy prowadzący sprawy majątkowe. Należy jednak pamiętać, że gdy zajdzie taka konieczność należy wystąpić o przyznanie pracownikom uprawnień do JPK_Lunetka.

Uwzględniono także wyjaśnienia NUS dot. nienadania pracownikowi SKA-2 uprawnień do WRO-System[8].

W skontrolowanym zakresie stwierdzono następujące uchybienia:

- Dane w Qasystent nie odpowiadały faktycznie nadanym uprawnieniom do systemów informatycznych – dotyczy to m.in. uprawnień do WRO-System. Brak odzwierciedlenia wszystkich uprawnień nadanych do systemów informatycznych. W toku kontroli uzupełniono braki i uaktualniono zapisy w Qasystent w tym zakresie. Nie odnotowano w Qasystent nadania dostępu (uprawnień) do e-ORUS (potwierdzenie nadania uprawnień do tej aplikacji) oraz CSU (odnotowanie roli do aplikacji Portal CSU).
- Nie odebrano uprawnień w CSU długotrwale nieobecnemu pracownikowi.
- Pracownicy posiadali nadmiarowe uprawnienia do systemów informatycznych (Qasystent, SSP) – po zmianie zakresu realizowanych zadań na danym stanowisku.

Nie stwierdzono, aby ww. uchybienia wywołały negatywne skutki dla kontrolowanej jednostki. Należy zauważyć, że w części przypadków NUS jeszcze przed rozpoczęciem kontroli instytucjonalnej, podczas prowadzonych przeglądów uprawnień usunął część błędów. W pozostałym zakresie wystąpił o uaktualnienie uprawnień w toku czynności kontrolnych DIAS, co oceniono pozytywnie.

Przegląd uprawnień

Zgodnie z treścią Procedury zarządzania uprawnieniami do systemów informatycznych[9] stanowiącej załącznik nr 1 do Instrukcji Zarządzania Systemami Informatycznymi, kierownicy komórek organizacyjnych jednostki nie rzadziej niż raz na pół roku dokonują przeglądu zasadności i aktualności uprawnień nadanych podległym pracownikom.

[8] Na dzień zakończenia kontroli pracownik nie obsługuje już NUS w Ostrowie Wielkopolskim.

[9] Zarządzenie Nr 250/2022 Dyrektora Izby Administracji Skarbowej w Poznaniu z dnia 30 grudnia 2022 r. w sprawie Systemu Zarządzania Bezpieczeństwem Informacji i polityk bezpieczeństwa w Izbie Administracji Skarbowej w Poznaniu.

Tożsame regulacje wynikają z Zarządzenia Nr 127/2018 Dyrektora Izby Administracji Skarbowej w Poznaniu z dnia 28 września 2018 r. w sprawie wykorzystania systemu Qasystent do realizacji procesu zarządzania uprawnieniami do systemów informatycznych funkcjonujących w Izbie Administracji Skarbowej w Poznaniu. Dyrektor DIAS w Poznaniu nakazał w nim przeprowadzanie, minimum raz na pół roku, kontroli w zakresie przydzielenia uprawnień do systemów informatycznych (…) - § 10 ust. 1 Zarządzenia.

Przeglądu zasadności i aktualności uprawnień do systemów informatycznych nadanych podległym pracownikom kierownicy w kontrolowanej jednostce dokonywali, co do zasady dwa razy w roku. Stwierdzono jednak przypadki weryfikacji jeden raz w roku lub brak dokonania takiego przeglądu:

- Komórka SPO w 2024 r. – jeden przegląd uprawnień z 30 grudnia 2024 r.,
- Komórka SKA-2 w latach 2019-2020 r. brak przeglądu – wyjaśniono, że (…) objął komórkę 12 listopada 2019 r.; w 2020 r. przeglądu uprawnień dokonywał na bieżąco (wg wyjaśnienia pracownicy mieli nadane uprawnienia w zakresie pozwalającym na przeprowadzanie czynności sprawdzających w obszarze podatku dochodowego), w następnych latach przeglądy były dokumentowane i ewidencjonowane w SZD;
- Komórka SKP – w latach 2019-2022 brak przeglądu, w 2024 r. jeden przegląd uprawnień.
- ZN1 i ZN2 w 2021 r. brak przeglądu.

Brak przeprowadzenia przeglądu aktualności i zasadności nadanych uprawnień w wymaganych terminach stanowi uchybienie.

W związku z wymienionymi wcześniej rozbieżnościami w zakresie danych wykazanych w Qasystent, a faktycznie nadanymi pracownikom uprawnieniami istnieje ryzyko, że prowadzona weryfikacja była nierzetelna.

Nadzór nad aktualnością uprawnień jest procesem ciągłym. Na bieżąco należy nadzorować kwestie odebrania uprawnień:

- pracownikom nieobecnym przez dłuższy czas (powyżej 3 miesięcy),
- pracownikom, z którym rozwiązano stosunek pracy,
- pracownikom zmieniającym miejsce zatrudnienia (odebranie poprzednich i nadanie nowych uprawnień wymaganych dla nowego zakresu obowiązków).

Oprócz tego wymagana jest raz na pół roku kompleksowa weryfikacja uprawnień nadanych podległym pracownikom pod kątem ich zasadności i aktualności. Konieczne jest w tym przypadku pisemne jej udokumentowanie np. w ramach kontroli funkcjonalnej.

Ustalenia kontroli DIAS w Poznaniu wskazują, że dokonywana weryfikacja była nieskuteczna i/lub nierzetelna, o czym świadczy m.in. nadanie nadmiarowych uprawnień do systemów, niewykorzystywanych na danym stanowisku pracy, brak odwzorowania w Qasystent nadanych uprawnień do systemów np. WRO-System.

Przyczyną stwierdzonych błędów w zakresie uprawnień do systemów informatycznych było najczęściej niedopatrzenie, ale też wadliwe (nierzetelne) przeprowadzenie przeglądu uprawnień.

W zakresie braku prowadzenia przeglądów raz na pół roku przyczyną była niewłaściwie przyjęta praktyka przez Urząd.

Upoważnienia

Naczelnik Urzędu Skarbowego w Ostrowie Wielkopolskim nie uregulował kwestii upoważnień i pełnomocnictw, w wewnętrznych procedurach postępowania. Stosowano regulacje wydane przez Dyrektora Izby Administracji Skarbowej w Poznaniu.

Badaniem objęto 5 upoważnień udzielonych pracownikom US w Ostrowie Wielkopolskim, aktualnych na dzień 31 grudnia 2024 r. do załatwiania spraw i/lub podpisywania pism z up. NUS.
Upoważnienia zawierają prawidłową podstawę prawną. Zostały podpisane przez Naczelnika Urzędu Skarbowego w Ostrowie Wielkopolskim. Odbiór upoważnień pracownicy potwierdzili podpisem ze wskazaniem daty. Upoważnienia zostały zaewidencjonowane w prowadzonym w formie elektronicznej rejestrze upoważnień. Upoważnienia ewidencjonowane były chronologicznie. W 2024 r. upoważnienia ewidencjonowane były także w SZD.
W rejestrze za 2024 r. w części przypadków nie odnotowano konkretnej daty utraty mocy upoważnień, a jedynie podano przyczynę np. odwołanie ze stanowiska ZNUS, powołanie na stanowisko NUS itp. Powyższe nie dotyczyło sytuacji wydania nowego upoważnienia i związanej z tym utraty mocy poprzedniego (w tym przypadku prawidłowo odnotowywano datę utraty mocy upoważnienia).
W 1 przypadku w tabeli widnieje nieprawidłowe nazwisko osoby, której dotyczy upoważnienie[10] (była to pomyłka pisarska – poz. 33 rejestru).
Jeszcze w toku kontroli błędy poprawiono (udostępniono do wglądu poprawiony rejestr upoważnień), co oceniono pozytywnie.

II. Wykorzystanie systemów informatycznych do celów służbowych

Na podstawie art. 35 ust. 1 pkt 1 ustawy o Krajowej Administracji Skarbowej organy KAS wykonują swoje zadania przy wykorzystaniu Centralnego Rejestru Danych Podatkowych (CRDP).

Przez CRDP[11] rozumie się system teleinformatyczny służący do:

1) gromadzenia, analizy oraz przetwarzania danych wynikających z:

a) deklaracji składanych przez podatników, płatników i ich następców prawnych,

b) decyzji, postanowień oraz innych dokumentów związanych z obowiązkami wynikającymi z przepisów prawa podatkowego i celnego,

c) tytułów wykonawczych i innych dokumentów przekazanych naczelnikowi urzędu skarbowego w celu realizacji jego zadań, o których mowa w art. 28 ust. 1 pkt 4,

ca) wyników analizy ryzyka, o której mowa w art. 119zn § 1 Ordynacji podatkowej, a także danych oraz dokumentów z nimi związanych, o których mowa w dziale IIIB Ordynacji podatkowej,

d) innych dokumentów i informacji przekazanych organom KAS w celu realizacji zadań ustawowych,

e) ewidencji, o których mowa w art. 109 ust. 3 i ust. 11g ustawy z dnia 11 marca 2004 r. o podatku od towarów i usług (Dz.U. z 2025 r. poz. 775, 894 i 896),

f) Krajowego Systemu e-Faktur, o którym mowa w ustawie z dnia 11 marca 2004 r. o podatku od towarów i usług,

g) ewidencji, o której mowa w art. 110b ust. 1 ustawy z dnia 11 marca 2004 r. o podatku od towarów i usług,

h) pism w sprawie korzystania przez podatnika ze zwolnienia od podatku od towarów i usług, o którym mowa w art. 113b ustawy z dnia 11 marca 2004 r. o podatku od towarów i usług;

2) przetwarzania danych zgromadzonych w Centralnym Rejestrze Podmiotów - Krajowej Ewidencji Podatników, a także danych pozyskanych z baz, rejestrów, ewidencji, zbiorów i systemów informatycznych udostępnionych organom KAS w celu realizacji ustawowych zadań.

[10] Jest (...) powinno być (...).
[11] Art. 35 ust. 3 ustawy o KAS.

Zgodnie z art. 45 ust. 1 ustawy o Krajowej Administracji Skarbowej, Organy KAS, w celu realizacji ustawowych zadań w zakresie, o którym mowa w art. 2 ust. 1 pkt 1, 2, 6, 8, 10, 13-15, 17a i 20a, mogą przetwarzać informacje, w tym dane osobowe, od osób prawnych, jednostek organizacyjnych niemających osobowości prawnej oraz osób fizycznych prowadzących działalność gospodarczą, o zdarzeniach mających bezpośredni wpływ na powstanie lub wysokość niepodatkowych należności budżetowych, zobowiązania podatkowego lub należności celnych, o zdarzeniach wynikających ze stosunków cywilnoprawnych lub faktycznych czynności mogących mieć wpływ na powstanie obowiązku podatkowego lub wysokość zobowiązania podatkowego, a także występować do tych podmiotów o udostępnienie dokumentów zawierających informacje, w tym dane osobowe.

W myśl art. 47b ust. 1 ustawy o KAS [Zasady przetwarzania danych osobowych] Organy KAS przetwarzają dane osobowe, w tym w CRDP, w celach realizacji zadań lub obowiązków określonych w ustawie, przez okres niezbędny do osiągnięcia tych celów.

Zgodnie z art. 47e ww. ustawy dane osobowe przetwarzane w celu wykonywania zadań wynikających z ustawy podlegają zabezpieczeniom zapobiegającym nadużyciom lub niezgodnemu z prawem dostępowi lub przekazywaniu polegającym co najmniej na:

1) dopuszczeniu przez administratora danych do przetwarzania danych osobowych wyłącznie osób do tego uprawnionych;

2) pisemnym zobowiązaniu osób upoważnionych do przetwarzania danych osobowych do zachowania ich w tajemnicy;

3) regularnym testowaniu i doskonaleniu stosowanych środków technicznych i organizacyjnych;

4) zapewnieniu bezpiecznej komunikacji w sieciach teleinformatycznych, w szczególności poprzez zagwarantowanie, by proces pozyskiwania i przekazywania danych osobowych podmiotom zewnętrznym wykorzystywał techniki kryptograficzne;

5) zapewnieniu ochrony przed nieuprawnionym dostępem do systemów informatycznych KAS;

6) zapewnieniu integralności danych w systemach informatycznych KAS;

7) określeniu zasad bezpieczeństwa przetwarzanych danych osobowych.

Systemy informatyczne mogą służyć pracownikom KAS wyłącznie do realizacji zadań służbowych. W praktyce oznacza to, że dane mogą być przeglądane i wykorzystywane wyłącznie w związku z prowadzoną przez pracownika sprawą. Niedopuszczalne jest wykorzystywanie danych do innych celów niż wynikających z prowadzonych spraw.

W ramach kontroli dokonano oceny w zakresie następujących zasad Systemu Zarządzania Bezpieczeństwem Informacji:

- Zasada przywilejów koniecznych – każda osoba posiada prawa dostępu do informacji ograniczone wyłącznie do tych, które są konieczne do wykonywania powierzonych mu zadań.
- Zasada wiedzy koniecznej – każda osoba posiada wiedzę o zasobie, do którego ma dostęp ograniczoną wyłącznie do zagadnień, które są konieczne do realizacji powierzonych zadań.
- Zasada indywidualnej odpowiedzialności – każda osoba odpowiada za bezpieczeństwo poszczególnych zasobów.
- Zasada ochrony danych osobowych – dane osobowe mogą być przetwarzane wyłącznie zgodnie

z prawem. Przetwarzanie danych w sposób inny niż określony w przepisach prawa stanowi naruszenie bezpieczeństwa informacji.

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

W kwestii rozliczalności – administrator jest odpowiedzialny za przestrzeganie ww. zasad oraz musi być w stanie wykazać ich przestrzeganie. Oznacza to, że w ramach realizacji uprawnień kontrolnych osób, których dane dotyczą, a także organu nadzorczego istnieje możliwość „rozliczenia" administratora oraz jego podwładnych.

Naczelnik Urzędu Skarbowego w Ostrowie Wielkopolskim w piśmie z 29 lipca 2025 r. poinformował, że w urzędzie nie stosowano mechanizmów, które pozwoliłyby na rozliczalność przeglądania/pobierania danych z realizowanymi czynnościami służbowymi. W przypadku dostępu limitowanego udostępnianie informacji w związku z prowadzoną sprawą mogło wynikać z zapytania mailowego, zapytań telefonicznych.

Kontroli poddano przeglądanie danych w systemach:

- Podatnik360,
- WRO-System,
- PoltaxPlus,

przez 19 pracowników kontrolowanego US (w tym pracowników komórek kontroli podatkowej, orzecznictwa oraz analiz i czynności sprawdzających, a także zastępców NUS).

Podatnik 360

Kontroli poddano 100 % populacji.

Z badanej próby 19 pracowników 8 przeglądało dane podmiotów w aplikacji Podatnik 360. Na 33 przypadki przeglądania danych, związek z prowadzonymi czynnościami służbowymi (prowadzonymi sprawami) istnieje w 27 przypadkach. W 6 przypadkach:

- (…) przeglądał swoje dane (4 przypadki przeglądania) oraz dane IAS w Warszawie (1 przypadek). Jako przyczynę przeglądania danych w Podatnik 360 podał przeglądanie możliwości aplikacji z wykorzystaniem podręcznika ze strony http://ckpp.mf.gov.pl/. Temu wyjaśnieniu nie dano wiary – dane przeglądano 31 października 2022 r., 20 lipca 2023 r., 29 lutego 2024 r., 1 marca 2024 r., 9 lutego 2024 r., czyli także w dużym odstępie czasu od wdrożenia aplikacji. Możliwości aplikacji są opisane właśnie w dokumencie „Podatnik360 Kompleksowy widok podatnika Instrukcja dla użytkownika do modułu Teczka podatnika" i to stamtąd należało czerpać wiedzę w tym zakresie.
- Pracownik (…) przeglądała dane męża (z którym wg wyjaśnienia pozostaje w związku małżeńskim). Jako przyczynę przeglądania danych męża w Podatnik 360 wskazała na chęć przetestowania systemu pod kątem widocznych w nim danych odnośnie do osób z inną właściwością miejscową. Takie działanie było również niewłaściwe – w tym przypadku brak związku przeglądania z przydzieloną do realizacji sprawą.

Działania w systemach muszą być rozliczalne i muszą mieć związek z prowadzoną przez pracownika sprawą. Wszelkie odstępstwa od tej zasady oceniane są negatywnie.

Reasumując, aplikację Podatnik 360 wykorzystano bez związku z prowadzonymi przez pracowników sprawami w 6 na 27 przypadków przeglądania (22 % populacji), co stanowi nieprawidłowość, za którą odpowiedzialność ponoszą pracownicy Urzędu Skarbowego w Ostrowie Wielkopolskim (…) i (…).

WRO-System[12]

Stwierdzono, że 4 pracowników z badanych 19 nie miało nadanych uprawnień do WRO-System, a 2 pracowników nie przeglądało danych we WRO-System mimo posiadania uprawnień.
Ustalono, że 13 pracowników w kontrolowanym okresie wyszukiwało we WRO-System, co najmniej 1 rekord. Poszczególni pracownicy przeglądali od 1 do 15535 rekordów[13].
W zakresie próby kontrolnej 58 przypadków przeglądania podmiotów przez 13 pracowników, stwierdzono, że tylko w 1 przypadku istnieją wątpliwości, co do zasadności przeglądania[14] (również kontrolowana jednostka w wyjaśnieniach wykazuje prawdopodobieństwo przeglądania). W 57 na 58 (98 % próby) wyszukiwania miały związek z realizowanymi czynnościami służbowymi (prowadzonymi sprawami), co oceniono pozytywnie.

Oprócz powyższego, na podstawie analizowanych danych stwierdzono przypadki przeglądania przez (…) podmiotów w module ANALIZER:

- ANALIZER Raporty analityczne - Pliki JPK,
- ANALIZER Raporty analityczne - Faktury zakupu,

w odstępach co kilka minut.

Przeglądanie dotyczyło różnych podmiotów. Przy czym dane (…) przeglądał (pobierał) z reguły w odstępach jedno, dwu lub trzyminutowych. Taki czas przeznaczony na analizę poszczególnej sprawy jest niewystarczający.

Do (…) zwrócono się o wyjaśnienie tej kwestii (jako przykład udostępniono przypadki przeglądania w ten sposób podmiotów z 4 kolejnych dni roboczych) i poinformowanie w jakim celu pracownik przeglądał/pobierał te dane oraz w jaki sposób zostały one wykorzystane do realizacji zadań służbowych.

(…) w wyjaśnieniu z 17 września 2025 r. wskazał, że korzystanie z WRO-System z modułu ANALIZER każdorazowo było związane tylko i wyłącznie z akceptacją zwrotów podatku VAT. Moduł był wykorzystywany do sprawdzenia zakupów u podatnika, u którego wystąpił zwrot VAT w korespondencji z wykazaniem przez wystawcę faktury konkretnej faktury VAT. (…) oświadczył także, że niejednokrotnie sprawdzał tylko czy łączna kwota zakupów wykazana w deklaracji VAT jest zgodna z kwotą wykazaną w przesłanym JPK_VAT. Sprawdzanie tylko łącznej kwoty zakupów wiązało się z pobieraniem danych w odstępach jedno, dwu lub trzyminutowych. Wg wyjaśnienia wykorzystanie przez ZNUS danych z modułu ANALIZER można powiązać z kartą analizy zwrotu VAT.

Odnosząc się do złożonego wyjaśnienia, analiza danych w systemach informatycznych tego nie potwierdza. Sprawdzono 10 wyszukiwań wykonanych 24 listopada 2023 r. w godzinach od 9:30 do 10:02[15].

[12] Ustaleń dokonano na podstawie informacji udzielonych przez komórkę ICK1 IAS w Poznaniu.
[13] Uwaga: jednego sprawdzanego podmiotu może dotyczyć wiele rekordów przeglądania.
[14] Przeglądanie 18 listopada 2022 r.
[15] Wśród nich występuje sprawdzenie grudnia 2018 r. – jest to okres domyślny i zapewne został wybrany omyłkowo, został on pominięty w analizie.

Wszystkie sprawdzenia[16] dotyczą października 2023 r., przy czym deklaracje VAT-7 zostały złożone 23 listopada 2023 r., a do PoltaxPlus zmigrowane w dniu następnym tj. 24 listopada 2023 r. Jako cel przeglądania wskazano: analiza, źródło: CHD.

Stwierdzono, że w żadnym z 10 badanych przypadków w deklaracjach za październik 2023 r. podatnicy nie wykazali nadwyżki podatku naliczonego nad należnym do zwrotu. Należy zauważyć, że ewentualna analiza zgodności kwot z części deklaracyjnej i ewidencyjnej JPK_V7M nie należała do (…), a do innych pracowników US.

Zatem wyjaśnienia (…) są niewiarygodne w zakresie przeglądania analiz podmiotów z WRO-System w odstępach co kilka minut. (…) nie wykazał związku przeglądania z realizacją powierzonych zadań. Brak rozliczalności polegający na wykonywaniu w służbowych systemach informatycznych zapytań bądź sprawdzeń osób lub podmiotów niezwiązanych z wykonywanymi zadaniami służbowymi w zakresie przeglądania danych we WRO-System stanowi nieprawidłowość, za którą odpowiada (…).

PoltaxPlus

Zbadano przeglądanie przez 16 pracowników danych (informacji) dotyczących 169 osób fizycznych[17]:

1. (…) – przeglądanie danych 13 osób,
2. (…) – przeglądanie danych 12 osób.
3. (…) – przeglądanie danych 5 osób.
4. (…) – przeglądanie danych 5 osób.
5. (…) – przeglądanie danych 5 osób.
6. (…) – przeglądanie danych 14 osób.
7. (…) – przeglądanie danych 10 osób.
8. (…) – przeglądanie 6 osób.
9. (…) – przeglądanie 6 osób.
10(…) – przeglądanie 1 osoby.
11. (…) – przeglądanie 30 osób,
12. (…) – przeglądanie 8 osób,
13. (…) – przeglądanie 21 osób,
14. (…) – przeglądanie danych 26 osób,
15. (…) – przeglądanie danych 6 osób,
16. (…) – przeglądanie danych 1 osoby.

Związek przeglądania z realizowanymi przez pracowników sprawami wykazano w stosunku do 89 na 169 osób fizycznych:

1. (…) – 11 osób,
2. (…)– nie wykazano związku,
3. (…) – 5 osób,
4. (…) – 5 osób,
5. (…) – 4 osoby,
6. (…) – 9 osób,
7. (…) – 6 osób,
8. (…) – 6 osób,

[16] NIP: (…); (…); (…); (…); (…); (…); (…); (…); (…); (…).

[17] Przy doborze próby uwzględniono ryzyko przeglądania danych osób spokrewnionych oraz innych pracowników US w Ostrowie Wielkopolskim.

9. (…) – 2 osoby,
10. (…) – 1 osoba,
11. (…) – 10 osób,
12. (…) – 5 osób,
13. (…) – 2 osoby,
14. (…) – 17 osób,
15. (…) – 5 osób,
16. (…) – 1 osoba.

Należy jednak odnotować, że w niektórych przypadkach związek przeglądania z realizowanymi czynnościami służbowymi budzi wątpliwość np.:

- (…), przeglądała dane nieżyjącego już w chwili przeglądania podatnika, jak wyjaśniła w związku z telefonicznym skontaktowaniem się z nią wdowy po ww., która była jej osobiście znana. Na okoliczność udzielenia informacji nie został sporządzony żaden dokument.

  Odnosząc się do złożonego wyjaśnienia, skoro przeglądano konkretne dane to istnieje ryzyko, że zakres udzielonej odpowiedzi przekraczał zwykłe informacje i wymagał uwierzytelnienia dzwoniącej. Nie należy dopuszczać do wątpliwości w zakresie celu przeglądania i wykazania związku przeglądania z przydzielonymi do realizacji sprawami. W tym przypadku ponieważ przeglądanie danych dotyczyło osoby zmarłej nie doszło do naruszenia przepisów RODO.

- (…), przeglądała dane znanej sobie osoby, wg wyjaśnienia podatniczka poprosiła o sprawdzenie danych adresowych widniejących w systemie urzędu, z uwagi na to, że zmieniała w roku objętym rozliczeniem adres zamieszkania, przebywała w ośrodku dla osób chorych, po opuszczeniu ośrodka zamieszkała u swojej córki, stąd pojawiła się wątpliwość odnośnie do zgłoszonego adresu i problem (wg przekazanych informacji) z weryfikacją zeznania podczas wysyłki elektronicznej. Pracownik poinformował, że udzielił ww. informacji w dobrej wierze wiedząc, że podatniczka z uwagi na zły stan zdrowia nie jest w stanie pojechać do US i wyjaśnić tych wątpliwości. W zakresie przeglądania danych osobowych tej osoby to mimo, że według wyjaśnienia prowadzone było na prośbę podatnika, to jednak sposób realizacji był niewłaściwy. Już fakt, że była to osoba znana (…) budzi wątpliwości. Ponadto w zeznaniu składanym w formie elektronicznej podaje się dane rejestracyjne, na podstawie których następnie zmieniane są dane w systemach informatycznych, zatem weryfikacja adresu nie była w tym wypadku konieczna.

W 9 przypadkach na 169 (5 % próby) nie wykazano jednoznacznie, że przeglądanie danych miało związek z czynnościami służbowymi (realizowaną sprawą):

1. (…) – 1 osoba - z uwagi na odległy termin trudno pracownikowi jednoznacznie wskazać w ramach jakich czynności służbowych była informacja o podatniku wyświetlana. Prawdopodobnie było to wykorzystane w ramach czynności sprawdzających przy weryfikacji ulgi prorodzinnej. Matka dziecka korzystała z takiej ulgi, a ojciec był sprawdzany pod kątem skorzystania z ulgi na dziecko. Informacja ta była wykorzystywana w ramach realizowania zadań służbowych.
   Odnosząc się do złożonego wyjaśnienia, dane z systemów informatycznych, wskazują, że podatnik nie wykazywał takiej ulgi. We wcześniejszych okresach rozliczał się z żoną[18], ale aktualnie brak informacji, że osoby te nadal są małżeństwem (różne adresy zamieszkania).

[18] Podatniczka nie wykazywała ulgi prorodzinnej.

W tej sprawie pracownik nie wykazał jednoznacznie, że przeglądanie było realizowane w związku z czynnościami służbowymi (prowadzoną sprawą).

2. (…) – 3 osoby – wyjaśnienia złożył (…) (nieobecność pracownika) - pracownik zajmuje się sprawami dot. podatku od spadków i darowizn. Prowadzenie tych spraw wiąże się z koniecznością ustalenia kręgu osób zobowiązanych podatkowo, co wiąże się z konieczności weryfikacji danych dotyczących spadkodawców oraz spadkobierców (brak PESEL, brak adresu). W takich przypadkach, aby prawidłowo zidentyfikować osoby wskazane w orzeczeniu niezbędne jest sięganie do różnych systemów informatycznych i porównywanie dostępnych danych. Dodatkowo pracownik pełnił dyżury na Sali Obsługi Podatnika udzielając informacji podatnikom w zakresie podatków majątkowych. W związku z nieobecnością pracownika brak możliwości jednoznacznego ustalenia spraw, których dotyczyło przeglądanie.
3. (…) – 2 osoby - rozbieżność pomiędzy datami przeglądania a czynnościami realizowanymi wobec podatników w US.
4. (…) – 1 osoba - ze względu na upływ czasu od daty przeglądania w 2019 r. brak możliwości ustalenia jakiej sprawy dotyczyło przeglądanie.
5. (…) – 4 osoby – w 3 przypadkach pracownik nie przypomina sobie czego mogło dotyczyć przeglądanie danych tych osób, w 1 przypadku wyjaśnienia nie są spójne ze stanem faktycznym wynikającym z danych w systemach informatycznych, ponadto nie przedstawiono, żadnych dowodów na przeprowadzenie analizy, o której mowa w wyjaśnieniu.

We wskazanych wyżej przypadkach uwzględniono wyjaśnienia kontrolowanej jednostki. Ze względu na czasookres objęty kontrolą (lata 2019-2024) istnieje trudność w zakresie jednoznacznego ustalenia związku przeglądania z realizowanymi czynnościami służbowymi. Ponieważ dotyczy to 5 % badanej próby uznano to jako dopuszczalne.

Stwierdzono brak związku przeglądania danych z przydzielonymi do realizacji zadaniami służbowymi w 71 na 169 przypadkach przeglądania:

1. (…) – 2 osoby (15 % próby), z tego swoje dane oraz w 1 przypadku wg wyjaśnienia błędnie wybrany podmiot – zbieżność nazwisk.
2. (…) – 12 osób (100 % próby), z tego 9 osób w ramach przygotowania do działalności trenerskiej, 3 osoby (podwładni) w celu pozyskania danych kontaktowych,
3. (…) – 5 osób (35 % próby), wszystkie z rodziny,
4. (…) - 4 osoby (40 % próby), z tego swoje dane, w 1 przypadku byłego pracownika US, w 1 przypadku zmarłego współpracownika, w 1 przypadku współpracownika (pozyskanie danych kontaktowych),
5. (…) – 1 osoba (17 % próby) - swoje dane,
6. (…) – 18 osób (60 % próby), w tym swoje dane, dane osób z rodziny (a w 1 przypadku dane osoby o imieniu i nazwisku zbieżnym z siostrą), opisane w wyjaśnieniu jako obsługa podatników na Sali obsługi, lecz przeglądanie danych miało miejsce poza godzinami obsługi podatników, dane 7 współpracowników wg wyjaśnienia obsługiwanych na Sali obsługi (5 nie potwierdziło jednoznacznie, że byli obsługiwani w tym czasie na Sali obsługi, a 2 osoby zaprzeczyły), dane 3 współpracowników (wyszukiwanie kontaktu do pracowników),
7. (…) – 2 osoby (25 % próby), dane swoje i męża,
8. (…) – 19 osób (90 % próby), dane swoje i rodziny (co najmniej 6 osób), 5 współpracowników, pozostałe przeglądane osoby, co do których nie uzasadniono celu przeglądania (prowadzonej przez

pracownika sprawy),

9. (…) – 5 osób (19 % próby), w tym dane swoje i swojej rodziny (3 osoby), dane 2 współpracowników,
10. (…) – 1 osoba (17 % próby) - nieżyjący współpracownik.

Ustalono, że bez związku z realizacją przydzielonych spraw przeglądano dane osób/podmiotów w liczbie przekraczającej zakładane kryteria kontroli[19], co oceniono negatywnie.

Jako przyczynę wskazywano:

a) cele prywatne:

- sprawdzanie nr PESEL osoby przeglądającej lub członków bliższej i dalszej rodziny (według wyjaśnień na prośbę tych osób),
- sprawdzanie dochodów do oświadczenia majątkowego, informacji o dochodach do KZP,
- sprawdzanie poprawności składanych przez osoby z rodziny deklaracji podatkowych,
- pozyskanie danych kontaktowych do współpracowników lub byłych współpracowników (adresów, numerów telefonów),
- sprawdzenie daty śmierci byłych pracowników,
- sprawdzenie daty śmierci teścia do ubezpieczenia,

b) przygotowanie do działalności trenerskiej (prowadzenia szkoleń),

c) pomyłkowe wybranie podmiotu (m.in. zbieżność nazwisk),

d) czynności służbowe, jednak analiza danych tego nie potwierdza np.:

- obsługa podatników na Sali obsługi przed godzinami obsługi podatników, a także przed rozpoczęciem pracy Urzędu Skarbowego,
- obsługa współpracowników na Sali obsługi (żaden z pracowników nie potwierdził, że był w tym dniu obsługiwany na Sali),
- obsługa współpracownika na Sali obsługi w sytuacji, gdy przeglądający nie był już zatrudniony w komórce SOB,
- brak odnotowania w systemach spraw prowadzonych wobec podatników oraz brak wskazania konkretnych spraw, w których podmiot był przeglądany[20].

Dostęp do danych musi wynikać z przydzielonej do prowadzenia sprawy służbowej. Wykorzystanie danych z systemów informatycznych w innych celach jest niedopuszczalne (nieprawidłowość).

Należy zauważyć, że nieprawidłowość stanowi również nieuprawnione zapoznanie się z danymi osobowymi. Powyższe oceniono negatywnie również w kontekście przeglądania danych współpracowników.

W badanej próbie wystąpiły przypadki przeglądania danych osób fizycznych w związku z przygotowaniem do działalności trenerskiej. W tym zakresie w toku kontroli DIAS w Poznaniu wystąpił o zajęcie stanowiska do Departamentu Poboru Podatków MF.

DPP wypowiedział się jednoznacznie, że przeglądanie informacji o podatnikach będących we właściwości urzędu skarbowego, w stosunku do których nie podejmowano żadnych czynności służbowych jest niedopuszczalne. System PoltaxPlus posiada własne środowisko testowe, które zasadniczo jest odzwierciedleniem środowiska produkcyjnego. W środowisku testowym znajdują się dane testowe, które można wykorzystać do weryfikacji prawidłowości działania systemu (np. walidacji

[19] Ponad 30 % próby kontrolnej.

[20] Dane mogły być przeglądane w związku ze sprawą u innego podmiotu i dotyczyć np. danych kontrahenta, jednak w wyjaśnieniach tego nie wykazano.

poprawności wyników). Z uwagi na powyższe przygotowanie do realizacji szkolenia powinno być realizowane za pomocą tylko i wyłącznie środowiska testowego.[21] Należy dodać, że pracownik nie posiadał zgody Naczelnika Urzędu Skarbowego, ani bezpośredniego przełożonego na przeglądanie danych w systemie informatycznym w związku z przygotowaniem do prowadzenia szkoleń (działalność trenerska).

Składane przez pracowników Urzędu Skarbowego w Ostrowie Wielkopolskim wyjaśnienia wskazują na swobodne podejście do przeglądania informacji w systemach informatycznych, w szczególności danych osób z rodziny, współpracowników, swoich danych. Pracownicy wykorzystywali systemy informatyczne do celów prywatnych. Informacje, które wg wyjaśnień sprawdzali, były dostępne w inny sposób np. numery PESEL są zapisane w dokumentach (m.in. dowód osobisty), data zgonu wynika z aktu zgonu, który notabene należy okazać do wypłaty odszkodowania z ubezpieczenia. W kwestii spisania dochodów w celu złożenia oświadczenia przez pracownika, to w większości przypadków pracownicy posiadają w domach kopie dokumentów (np. PIT-11, zeznań rocznych itp.), a jeżeli utracili do nich dostęp to mogli wystąpić do Urzędu o wydanie kopii zeznania lub do pracodawcy o wydanie kopii PIT-11. Należy zauważyć, że od kilku lat dostęp do informacji o dochodach PIT-11 jest z poziomu aplikacji SYKAP (począwszy od PIT-11 za 2022 r.).
Zgodnie z art. 130 § 1 pkt 3 O.p. pracownik izby administracji skarbowej podlega wyłączeniu od udziału w postępowaniu w sprawach dotyczących zobowiązań podatkowych oraz innych spraw normowanych przepisami prawa podatkowego, w których stroną jest ich małżonek, rodzeństwo, wstępny, zstępny lub powinowaty do drugiego stopnia. Dlatego też każde przeglądanie danych dotyczących ww. osób należy rozpatrywać w kontekście obowiązku wyłączenia się pracownika z prowadzenia takich spraw (skoro niedopuszczalne jest prowadzenie przez pracowników spraw dotyczących ww. osób, wykluczona jest także możliwość przeglądania ich danych w systemach informatycznych).
Pracownicy działali wbrew zasadom bezstronności i rzetelności, o których mowa w Zarządzeniu Nr 70 Prezesa Rady Ministrów w sprawie wytycznych w zakresie przestrzegania zasad służby cywilnej oraz w sprawie zasad etyki korpusu służby cywilnej z dnia 6 października 2011 r. (M.P. Nr 93, poz. 953):

> § 18 Zasada bezstronności wyraża się w szczególności w:
> 1) niedopuszczaniu do podejrzeń o konflikt między interesem publicznym i prywatnym (…)
> § 19 Zasada rzetelności wyraża się w szczególności w:
> 1) sumiennym, rozważnym wykonywaniu powierzonych zadań;

Nieakceptowalne jest wykorzystywanie danych w systemach do przeglądania danych osób, wobec których pracownik nie prowadzi spraw. W związku z tym ustalanie adresów podwładnych na podstawie PoltaxPlus, w celu np. dostarczenia dokumentów do pracy zdalnej, oceniono jako niewłaściwe. W tym przypadku adresy, jeżeli była taka konieczność można było ustalić na podstawie wniosków o pracę zdalną składanych przez pracowników (konieczność zadeklarowania miejsca wykonywania pracy zdalnej, które notabene mogło być niezgodne z adresami zgłoszonymi w PoltaxPlus). Podobnie wyszukiwanie kontaktu do pracowników i byłych pracowników. Wyjaśnienia, że chciano skontaktować się w celach służbowych z byłym pracownikiem – obecnie świadczącym pracę w innym US – są niewiarygodne. Na stronie intranetowej IAS jest i była dostępna książka telefoniczna umożliwiająca ustalenie telefonu służbowego. Kontakt możliwy był także za pośrednictwem adresu e-mail (książka adresowa dostępna w Outlook'u). Niewłaściwe jest również kontaktowanie się w sprawach służbowych z pracownikiem przebywającym na zwolnieniu chorobowym.

[21] Pismo MF Departament Poboru Podatków z 24 października 2025 r. znak sprawy: DPP5.0723.17.2025.

Realizowane w celu prywatnym przeglądanie danych mające na celu pozyskanie informacji dotyczących np. PESEL-u syna, szwagra, telefonu kontaktowego do teściowej, dochodów męża do oświadczenia np. ZFŚS jest naganne.

Negatywnie oceniono również przeglądanie danych osób z rodziny w celu sprawdzenia:

- poprawności złożonych dokumentów podatkowych osób z rodziny, przy czym na szczególną krytykę zasługuje przeglądanie danych w okresie wyłączenia z właściwości NUS w Ostrowie Wielkopolskim podmiotów przeglądanych,
- odnotowania w systemach, czy w związku z objęciem funkcji (…) przez przeglądającego nastąpiło odnotowane wyłączenie z właściwości US.

Pracownik nie może weryfikować poprawności składanych dokumentów podatkowych wobec członków jego rodziny, ponieważ budzi to wątpliwości, co do jego bezstronności. Należy tu zauważyć, że przeglądanie miało miejsce także w okresie, gdy członek rodziny był wyłączony z właściwości NUS w Ostrowie Wielkopolskim. (…) nie był uprawniony do weryfikacji czy nastąpiło już wyłączenie właściwości. Takie informacje mógł zweryfikować pracownik SKI lub np. Naczelnik US pod kątem odnotowania w systemach zmiany US.

Działania były realizowane bez związku z przydzielonymi zadaniami służbowymi tj. przeglądanie nie miało związku z prowadzoną sprawą, co oceniono negatywnie.

Należy zauważyć, że w części przypadków pracownicy wskazywali, że prowadzili wobec podmiotów czynności, nie okazali jednak na powyższe żadnych dowodów. Jeżeli prowadzono analizy to powinny one znaleźć swoje odzwierciedlenie w dokumentacji (raportach, rejestrach, adnotacjach, protokołach itp.).

W Urzędzie nie wypracowano zasad (metod), które pozwoliłyby na pełne wdrożenie zasady rozliczalności.

Podsumowując, stwierdzono nieprawidłowość polegającą na wykorzystywaniu systemów informatycznych do innych celów niż przydzielone do realizacji sprawy, co stanowi naruszenie:

1) Zasady bezstronności i rzetelności, o których mowa w Zarządzeniu Nr 70 Prezesa Rady Ministrów w sprawie wytycznych w zakresie przestrzegania zasad służby cywilnej oraz w sprawie zasad etyki korpusu służby cywilnej z dnia 6 października 2011 r. (M.P. Nr 93, poz. 953),

2) Przepisów 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) (Dz.Urz. UE L 119 z 04.05.2016, str. 1), w szczególności zasady przetwarzania danych osobowych (art. 5 rozporządzenia) i zgodności przetwarzania z prawem (art. 6 rozporządzenia).

W badanych przypadkach zaistniała możliwość bezprawnego przetwarzania danych osobowych. Do zdarzeń doszło wskutek świadomego działania pracowników przetwarzających dane.

3) Polityki Bezpieczeństwa Informacji Resortu Finansów, której naruszenie może wywołać określone skutki:

Zgodnie z § 24 Polityki Bezpieczeństwa Informacji Resortu Finansów:

1. Naruszenie bezpieczeństwa informacji może być uznane za ciężkie naruszenie obowiązków pracowniczych.
2. Niezastosowanie się do przepisów o ochronie informacji prawnie chronionych, a także do Polityki, polityk szczegółowych i procedur dotyczących ochrony informacji, może powodować odpowiedzialność karną, dyscyplinarną lub służbową.

4) Regulacji prawa wewnętrznego[22] Izby Administracji Skarbowej w Poznaniu w zakresie Systemu Zarządzania Bezpieczeństwem Informacji i polityk bezpieczeństwa w Izbie Administracji Skarbowej w Poznaniu, zgodnie z którym zabronione jest m.in. wyszukiwanie, przeglądanie, pobieranie danych z systemów informatycznych niezwiązanych z wykonywanymi czynnościami służbowymi[23].

Nieprzestrzeganie zasad określonych w dokumentach określających politykę bezpieczeństwa informacji stosowanych na danym stanowisku pracy przez użytkownika stanowi naruszenie podstawowych obowiązków pracowniczych i może podlegać odpowiedzialności dyscyplinarnej lub karnej[24].

W Urzędzie Skarbowym w Ostrowie Wielkopolskim nie przestrzegano zasad dotyczących bezpieczeństwa informacji:

- zasady wiedzy koniecznej – zgodnie z którą, pracownicy posiadają dostęp tylko do tych informacji, które są konieczne do realizacji powierzonych im zadań,
- zasady domniemanej odmowy – przyjęcia jako standardowych najbardziej restrykcyjnych ustawień, które można zwolnić jedynie w określonych sytuacjach[25],
- zasady ochrony danych osobowych – dane osobowe mogą być przetwarzane wyłącznie zgodnie z prawem. Przetwarzanie danych w sposób inny niż określony w przepisach prawa stanowi naruszenie bezpieczeństwa informacji.

Na podstawie próby kontrolnej stwierdzono możliwość naruszenia zasad bezpieczeństwa informacji poprzez niewłaściwe wykorzystanie zasobu. Zgodnie z zasadą indywidualnej odpowiedzialności za utrzymanie odpowiedniego poziomu bezpieczeństwa poszczególnych aktywów lub ich elementów odpowiadają konkretne osoby, w zakresie nałożonych obowiązków i nadanych uprawnień.
W kontrolowanej jednostce wystąpiło nadużycie posiadanych uprawnień w systemie PoltaxPlus związane z nadmiarowym przetwarzaniem danych osobowych w celach niezwiązanych z realizacją zadań służbowych[26].

[22] Zarządzenie Nr 250/2022 Dyrektora Izby Administracji Skarbowej w Poznaniu z dnia 30 grudnia 2022 r. w sprawie Systemu Zarządzania Bezpieczeństwem Informacji i polityk bezpieczeństwa w Izbie Administracji Skarbowej w Poznaniu; Zarządzenie Nr 12/2022 Dyrektora Izby Administracji Skarbowej w Poznaniu z dnia 16 lutego 2022 r. w sprawie ustanowienia i wdrożenia Systemu Zarządzania Bezpieczeństwem Informacji w Izbie Administracji Skarbowej w Poznaniu; Zarządzenie Nr 167/2019 Dyrektora Izby Administracji Skarbowej w Poznaniu z dnia 28 listopada 2019 r. w sprawie ustanowienia i wdrożenia Systemu Zarządzania Bezpieczeństwem Informacji w Izbie Administracji Skarbowej w Poznaniu; Zarządzenie Nr 122/2020 Dyrektora Izby Administracji Skarbowej w Poznaniu z dnia 4 września 2020 r. zmieniające zarządzenie w sprawie ustanowienia i wdrożenia Systemu Zarządzania Bezpieczeństwem Informacji w Izbie Administracji Skarbowej w Poznaniu; Zarządzenie Nr 159/2020 Dyrektora Izby Administracji Skarbowej w Poznaniu z dnia 24 listopada 2020 r. zmieniające zarządzenie w sprawie ustanowienia i wdrożenia Systemu Zarządzania Bezpieczeństwem Informacji w Izbie Administracji Skarbowej w Poznaniu.
[23] Patrz: Polityka Bezpieczeństwa Informacji IAS w Poznaniu - Regulamin użytkownika.
[24] Patrz: Polityka Bezpieczeństwa Informacji IAS w Poznaniu - Regulamin użytkownika.
[25] To, co nie jest dozwolone, jest zabronione.
[26] Zagrożenie: naruszenie bezpieczeństwa informacji – patrz: INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM POLTAXPLUS wraz z załącznikami.

W związku z powyższym istnieje ryzyko zakwalifikowania takiego przeglądania jako incydent bezpieczeństwa informacji, a w przypadku potwierdzenia jego wystąpienia zgłoszenie do Prezesa Urzędu Ochrony Danych Osobowych.

Stwierdzono także istnienie ryzyka naruszenia art. 130 O.p. § 1 pkt 3 O.p. przez pracowników (niewyłączenie się pracowników).
Osoby odpowiedzialne za stwierdzone nieprawidłowości w zakresie korzystania z systemu PoltaxPlus – pracownicy US w Ostrowie Wielkopolskim: (…), (…), (…), (…), (…), (…), (…), (…), (…), (…) oraz w trybie nadzoru kierownicy komórek organizacyjnych, Zastępcy NUS oraz Naczelnik Urzędu Skarbowego w Ostrowie Wielkopolskim.

Podsumowując, zagadnienie wykorzystania systemów informatycznych do celów służbowych oceniono negatywnie. Niewłaściwe działanie stwierdzono w stosunku do wszystkich badanych systemów informatycznych. Jednak najwięcej nieprawidłowości stwierdzono w zakresie wykorzystania systemu PoltaxPlus, w którym dane 71 osób fizycznych tj. 42 % próby przeglądano bez związku z realizowanymi czynnościami służbowymi. Również w pozostałych skontrolowanych systemach tj. WRO-System oraz Podatnik360 stwierdzono przypadki braku wykazania związku przeglądania z realizowanymi sprawami.
Wystąpiło nieuprawnione zapoznanie się z danymi osobowymi, naruszenie przepisów RODO, zasad bezstronności i rzetelności, o których mowa w Zarządzeniu Nr 70 Prezesa Rady Ministrów w sprawie wytycznych w zakresie przestrzegania zasad służby cywilnej oraz w sprawie zasad etyki korpusu służby cywilnej z dnia 6 października 2011 r. (M.P. Nr 93, poz. 953), przepisów prawa wewnętrznego, Polityki Bezpieczeństwa Informacji Resortu Finansów. Zgodnie z art. 33 ust. 1 RODO, w sytuacji gdy zaistniałe naruszenie skutkuje ryzykiem naruszenia praw lub wolności osób fizycznych, administratorzy zobligowani są do zgłoszenia naruszenia krajowemu organowi nadzorczemu, którym w Rzeczypospolitej Polskiej jest Prezes Urzędu Ochrony Danych Osobowych (Prezes UODO). Ponadto wobec osób przeglądających dane może zostać zastosowana odpowiedzialność dyscyplinarna.
W przypadku dostępu do danych z deklaracji (np. zeznań podatkowych) należy zwrócić uwagę na brzmienie przepisu art. 293 § 1 O.p., zgodnie z którym indywidualne dane zawarte w deklaracji lub innych dokumentach składanych przez podatników, płatników lub inkasentów objęte są tajemnicą skarbową. Pracownicy izb administracji skarbowej są zobowiązani do jej przestrzegania (art. 294 § 1 pkt 1 O.p.), a obowiązujące przepisy w zakresie złamania tajemnicy skarbowej (art. 306 § 1-4 O.p.), mogą skutkować odpowiedzialnością karną.

Stwierdzone w toku kontroli DIAS w Poznaniu nieprawidłowości mogą wywołać skutki aktualnie trudne do oszacowania, zarówno po stronie kontrolowanej jednostki, jak też po stronie osób przeglądających w sposób nieuprawniony dane.

III. Kontrola funkcjonalna

Kontrole funkcjonalne powinny być realizowane zgodnie z Procedurą kontroli funkcjonalnej wprowadzoną przez Dyrektora Izby Administracji Skarbowej w Poznaniu Zarządzeniem nr 167/2018 z dnia 15 grudnia 2018 r. w sprawie wprowadzenia kontroli funkcjonalnej, następnie zmienioną zarządzeniem nr 24/2019 z 25 marca 2019 r., nr 59/2019 z 27 maja 2019 r., nr 63/2020 z 17 lipca 2020 r.

i nr 211/2021 z 25 listopada 2021 r.[27]

Zgodnie z § 6 Procedury kontroli funkcjonalnej, informacje należy ewidencjonować w kategorii spraw o symbolu i haśle klasyfikacyjnym *093 – kontrola funkcjonalna.* W kontrolowanej jednostce na informacjach o prowadzonej kontroli funkcjonalnej nanoszony był numer z ww. kategorii spraw.

Kwestie aktualności i zasadności nadawanych uprawnień do systemów informatycznych zostały wyznaczone przez Dyrektora Izby Administracji Skarbowej w Poznaniu jako priorytet kierownictwa izby celem ich uwzględnienia w ramach wykonywania czynności kontroli funkcjonalnej.

Ustalenia dot. terminowości przeprowadzania kontroli funkcjonalnych w zakresie weryfikacji uprawnień do systemów informatycznych opisano we wcześniejszej części dokumentu.

Naczelnik Urzędu Skarbowego w Ostrowie Wielkopolskim złożył wyjaśnienia odnośnie do kontroli funkcjonalnych[28].

Kierownicy komórek oraz Zastępcy NUS prowadzili kontrole funkcjonalne obejmujące swoim zakresem kwestie aktualności i zasadności nadawania uprawnień do systemów informatycznych.

Przeprowadzone kontrole dokumentowano w Informacjach o przeprowadzonej kontroli funkcjonalnej.

Zapisy w ww. informacjach często były sformułowane ogólnie i nie wynikało z nich na podstawie jakich danych i z jakich systemów została przeprowadzona weryfikacja, uprawnienia jakich pracowników weryfikowano. Nie formułowano zaleceń pokontrolnych mimo stwierdzenia niezasadnie nadanych uprawnień lub stwierdzonej konieczności rozszerzenia uprawnień. Nie odnotowywano, czy i jakie uprawnienia po przeprowadzonej kontroli funkcjonalnej zostały pracownikom nadane lub odebrane.

Przy dokonywaniu przeglądu należało w informacji zawrzeć opis próby (badanych pracowników i przydzielonych im uprawnień – można było dołączyć wydruki w pdf z aplikacji Qasystent), zadania na stanowisku objętym kontrolą lub realizowane przez pracownika, wynik sprawdzenia pod względem aktualności i zasadności nadanych uprawnień, a także czy wszystkie uprawnienia zostały odzwierciedlone w Qasystent, zalecenia i termin ich realizacji. Wymagane było także odnotowanie informacji o realizacji zleceń pokontrolnych.

Należy zwrócić uwagę, aby wszystkie informacje o przeprowadzonej kontroli funkcjonalnej były zaewidencjonowane w SZD wraz z załącznikami. Tylko kompletna informacja daje zapewnienie, że kontrola funkcjonalna została przeprowadzona rzetelnie i starannie.

W niniejszej kontroli ustalono m.in. brak odzwierciedlenia nadanych uprawnień w Qasystent, w związku z tym kontrole prowadzone w oparciu o raporty/wydruki z tego systemu mogły być nierzetelne, a sformułowane wnioski niewiarygodne.

W zakresie prowadzonych kontroli funkcjonalnych stwierdzono, że dokumentacja i ustalenia z kontroli funkcjonalnych nie dawała rękojmi, że pracownicy posiadają aktualne i adekwatne do wykonywanych zadań uprawnienia do systemów informatycznych, co stanowi uchybienie.

Kwestia wykorzystania systemów informatycznych przez pracowników nie była przedmiotem weryfikacji w ramach kontroli funkcjonalnej, chociaż Naczelnik US mógł wystąpić np. do IAS o udostępnienie wykazów np. z Podatnik 360 (raporty audytowe) i WRO-System.

[27] Zgodnie z § 13 Procedury kontroli funkcjonalnej, komórka ds. kontroli wewnętrznej w dokumentach pokontrolnych, sporządzanych w wyniku przeprowadzonych kontroli wewnętrznych i instytucjonalnych, zawiera ocenę kontroli funkcjonalnych, przeprowadzonych w kontrolowanej jednostce w odniesieniu do obszaru objętego kontrolą.

[28] Pismo z 24 września 2025 r. 3017-SWW.0921.1.1.2025.19 (UNP 3001-25-174426).

Podsumowując kontrola funkcjonalna w kontrolowanym zakresie ograniczała się do weryfikacji aktualności i zasadności nadanych uprawnień do systemów informatycznych podległym pracownikom.

W skontrolowanym zakresie stwierdzono następujące nieprawidłowości (punkty od 1 do 3) i uchybienia (punkty od 4 do 7):

1. Przeglądane i wykorzystywanie danych w PoltaxPlus i Podatnik 360 bez związku z prowadzoną przez pracownika sprawą służbową, co stanowi naruszenie:

- Zasady bezstronności i rzetelności, o których mowa w Zarządzeniu Nr 70 Prezesa Rady Ministrów w sprawie wytycznych w zakresie przestrzegania zasad służby cywilnej oraz w sprawie zasad etyki korpusu służby cywilnej z dnia 6 października 2011 r. (M.P. Nr 93, poz. 953),
- Przepisów 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) (Dz.Urz. UE L 119 z 04.05.2016, str. 1), w szczególności zasady przetwarzania danych osobowych (art. 5 rozporządzenia) i zgodności przetwarzania z prawem (art. 6 rozporządzenia);
- Polityki Bezpieczeństwa Informacji Resortu Finansów;
- Regulacji prawa wewnętrznego Izby Administracji Skarbowej w Poznaniu w zakresie Systemu Zarządzania Bezpieczeństwem Informacji i polityk bezpieczeństwa w Izbie Administracji Skarbowej w Poznaniu, zgodnie z którym zabronione jest m.in. wyszukiwanie, przeglądanie, pobieranie danych z systemów informatycznych niezwiązanych z wykonywanymi czynnościami służbowymi.
- zasad dotyczących bezpieczeństwa informacji:
    - zasady wiedzy koniecznej,
    - zasady domniemanej odmowy,
    - zasady ochrony danych osobowych.

2. Brak rozliczalności polegający na wykonywaniu w służbowych systemach informatycznych zapytań bądź sprawdzeń osób lub podmiotów niezwiązanych z wykonywanymi zadaniami służbowymi w zakresie przeglądania danych we WRO-System.
3. Nieukończenie przez pracowników obowiązkowych szkoleń (Szkolenia RODO Unijne rozporządzenie o ochronie danych osobowych – 1 pracownik, szkolenie „Bezpieczeństwo teleinformatyczne – szkolenie dedykowane dla pracowników resortu finansów” – 4 pracowników).
4. Brak przeprowadzenia przeglądu aktualności i zasadności nadanych uprawnień w wymaganych terminach.
5. Realizacja obowiązkowych szkoleń z opóźnieniem.
6. Nieodebranie uprawnień w CSU długotrwale nieobecnemu pracownikowi.
7. Posiadanie przez pracowników nadmiarowych uprawnień do systemów informatycznych (Qasystent, SSP) – po zmianie zakresu zadań realizowanych na danym stanowisku.

Szczegółowy zakres, przyczyny i skutki stwierdzonych nieprawidłowości i uchybień, a w przypadku nieprawidłowości także osoby odpowiedzialne, zostały opisane w treści dokumentu.

Ocena skontrolowanego przedmiotu kontroli - negatywna.

[dowód: akta kontroli SZD poz. 20]

Informacja o zgłoszonych zastrzeżeniach do projektu wystąpienia pokontrolnego
Naczelnik Urzędu Skarbowego w Ostrowie Wielkopolskim nie wniósł zastrzeżeń do ustaleń kontroli zawartych w projekcie wystąpienia pokontrolnego.
Zalecenia i wnioski dotyczące usunięcia stwierdzonych nieprawidłowości lub usprawnienia funkcjonowania kontrolowanego urzędu
Dyrektor Izby Administracji Skarbowej w Poznaniu zaleca: 1. Wykorzystywać systemy informatyczne wyłącznie w związku z przydzieloną do prowadzenia sprawą. 2. Zapewnić rozliczalność w zakresie danych przeglądanych we WRO-System. 3. Wzmocnić nadzór nad realizacją obowiązkowych szkoleń przez podległych pracowników. 4. Prowadzić przeglądy aktualności i zasadności nadanych uprawnień do systemów informatycznych w wymaganych przepisami Dyrektora IAS w Poznaniu terminach. Weryfikację opierać na prawidłowych danych odzwierciedlonych we właściwych systemach (m.in. Qasystent, SZU). 5. Zapewnić terminową realizację obowiązkowych szkoleń przez pracowników. 6. Odbierać uprawnienia do systemów długotrwale nieobecnym pracownikom bez zbędnej zwłoki, w terminach wskazanych w przepisach prawa wewnętrznego. 7. Po zmianie zakresu zadań realizowanych na danym stanowisku dokonywać niezwłocznie weryfikacji pod kątem aktualności i zasadności nadanych uprawnień do systemów informatycznych. 8. Przeprowadzić kontrolę funkcjonalną w zakresie stwierdzonych nieprawidłowości i uchybień w terminie 9 miesięcy od dnia udzielenia informacji o sposobie wykonania zaleceń pokontrolnych oraz przekazać informację o rezultatach wdrożenia zaleceń pokontrolnych. 9.
Ocena wskazująca na niezasadność zajmowania stanowiska lub pełnienia funkcji przez osobę odpowiedzialną za stwierdzone nieprawidłowości
-
Pouczenie
Stosownie do przepisu art. 48 ustawy z dnia 15 lipca 2011 r. o kontroli w administracji rządowej (Dz. U. z 2020, poz. 224 ze zm.) w brzmieniu obowiązującym przed 6 września 2025 r., od wystąpienia pokontrolnego nie przysługują środki odwoławcze.
Termin złożenia informacji
W przypadku stwierdzonych uchybień bądź nieprawidłowości w terminie 30 dni od dnia otrzymania wystąpienia pokontrolnego należy poinformować Dyrektora Izby Administracji Skarbowej w Poznaniu o sposobie wykonania zaleceń, wykorzystaniu wniosków lub przyczynach ich niewykorzystania albo o innym sposobie usunięcia stwierdzonych nieprawidłowości, uchybień.

PODPIS DYREKTORA IZBY ADMINISTRACJI SKARBOWEJ
Dyrektor Izby Administracji Skarbowej w Poznaniu Maciej Młodzikowski (podpisano kwalifikowanym podpisem elektronicznym)
Kwalifikowany podpis elektroniczny ma skutek prawny równoważny podpisowi własnoręcznemu (art. 25 ust. 2 Rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE).

Korespondencję otrzymują

1. Adresat - elektronicznie
2. aa

Do wiadomości – wyłącznie drogą elektroniczną

1. Z-ca DIAS – Arkadiusz Radziejewski
2. Z-ca DIAS – Paweł Siuda
3. Z-ca DIAS – Robert Stangret
4. Z-ca DIAS – Dariusz Strugliński
5. Z-ca DIAS – Agata Wciórka
6. Wydział Kontroli Podatkowej, Kontroli Celno-Skarbowej i Nadzoru nad Czynnościami Sprawdzającymi oraz Zarządzania Ryzykiem (ICK)
7. Referat Nadzoru nad Orzecznictwem (ION)
8. Wieloosobowe Stanowisko Ochrony Danych (IWD)
9. Referat Bezpieczeństwa i Ochrony Informacji (IWO)
10. Dział Wsparcia Zarządzania oraz Statystyki i Analiz (IWZ)
11. Naczelnik Wydziału Egzekucji Administracyjnej oraz Nadzoru nad Rachunkowością Podatkową (IEE) – (…)