Krajowa Administracja Skarbowa

IZBA ADMINISTRACJI SKARBOWEJ W POZNANIU

Poznań, 21 lipca 2026 roku

UNP: 3001-26-104260

Znak sprawy: 3001-IWW1.0921.9.2026

Pan

Krzysztof Berlak
Naczelnik
Urzędu Skarbowego w Pleszewie
ul. Bogusza 6
63-300 Pleszew

SPRAWOZDANIE Z KONTROLI	
Sporządzone na podstawie art. 52 ust. 4 ustawy z dnia 15 lipca 2011 r. o kontroli w administracji rządowej (tj. Dz. U. z 2026 r., poz. 158)	
Nazwa i adres kontrolowanego urzędu	
3039 Urząd Skarbowy w Pleszewie **ul. Bogusza 6,** **63-300 Pleszew**	
Naczelnik kontrolowanego urzędu	
Pan Krzysztof Berlak	
Upoważnienie do przeprowadzenia kontroli	
Nr 14/2026 z 14 listopada 2026 r. wydane przez Dyrektora Izby Administracji Skarbowej w Poznaniu.	
Wpis do książki kontroli	
Kontrola w trybie uproszczonym wpisana pod pozycją nr 1/2026	
Koordynator kontroli – imię, nazwisko i stanowisko służbowe/stopień służbowy	
Magdalena Stejbach – główny ekspert skarbowy	
Kontrolerzy – imię, nazwisko i stanowisko służbowe/stopień służbowy	
1.	Magdalena Stejbach – główny ekspert skarbowy
Data rozpoczęcia czynności kontrolnych	15 kwietnia 2026 r.

Data zakończenia czynności kontrolnych	15 maja 2026 r.
Zakres kontroli	
Przedmiot kontroli	Uprawnienia do systemów informatycznych.
Okres objęty kontrolą	Od 1 stycznia 2025 r. do 31 grudnia 2025 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 (wg obszarów z kontrolowanego okresu). Zarządzanie bezpieczeństwem organizacji (obecnie).	
Cel kontroli	
Weryfikacja nadawania i rejestrowania uprawnień do systemów informatycznych, w przypadku zakończenia pracy lub długotrwałej absencji odbierania użytkownikom uprawnień do systemów informatycznych oraz ocena prawidłowości korzystania z systemów informatycznych do realizacji zadań służbowych.	
Ocena skontrolowanej działalności	
Pozytywna z nieprawidłowościami	
DOKONANE USTALENIA FAKTYCZNE	

I. Organizacja pracy urzędu w zakresie korzystania z systemów informatycznych

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

- Regulamin Organizacyjny stanowiący Załącznik nr 36/2024 z 23 kwietnia 2024 r. do Zarządzenia Dyrektora Izby Administracji Skarbowej w Poznaniu w sprawie nadania Regulaminu Organizacyjnego Urzędowi Skarbowemu w Pleszewie (obowiązujący do 31 maja 2025 r.)
- Regulamin Organizacyjny stanowiący Załącznik nr 62/2025 z 8 maja 2025 r. do Zarządzenia Dyrektora Izby Administracji Skarbowej w Poznaniu w sprawie nadania Regulaminu Organizacyjnego Urzędowi Skarbowemu w Pleszewie (obowiązujący od 1 czerwca 2025 r.)

Naczelnik Urzędu Skarbowego Pan Krzysztof Berlak realizuje zadania przy pomocy kierowników działów, kierowników referatów oraz kierujących wieloosobowymi stanowiskami.

Strukturę Urzędu Skarbowego tworzą komórki organizacyjne:

– Wieloosobowe Stanowisko Wsparcia (SWW),

– Referat Obsługi Bezpośredniej (SOB),

– Referat Postępowania Podatkowego (SPO),

– Referat Rachunkowości i Spraw Wierzycielskich (SER),

– Dział Czynności Analitycznych i Sprawdzających oraz Kontroli Podatkowej (SKA),

– Wieloosobowe Stanowisko Identyfikacji i Rejestracji Podatkowej (SKI).

Jak wynika z Regulaminów Organizacyjnych Urzędu Skarbowego w Pleszewie do zakresu zadań wszystkich komórek organizacyjnych należy w szczególności wykonywanie zadań w sposób zgodny z prawem, efektywny, oszczędny i terminowy.

Wskazują one także m.in. na realizację zadań z zakresu zarządzania kryzysowego, zarządzania ciągłością działania, obronności i bezpieczeństwa państwa oraz cyberbezpieczeństwa oraz przestrzeganie zasad bezpiecznego przetwarzania informacji.

Kierownicy komórek organizacyjnych nadzorują bezpośrednio i ponoszą odpowiedzialność za realizację zadań wynikających z Regulaminu w stosunku do podległych im pracowników.

Do zakresu odpowiedzialności kierowników komórek organizacyjnych należy m.in:

– przestrzeganie obowiązujących przepisów w zakresie tajemnicy służbowej i skarbowej, ochrony danych osobowych, bezpieczeństwa i higieny pracy, a także nadzorowanie w tym zakresie pracowników.

W okresie objętym kontrolą obowiązywały m.in.:

– Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych – RODO) (Dz. Urz. UE. L 119 z 4 maja 2016 r. Nr 119, str. 1 ze zm.), dalej rozporządzenie RODO,

– (…),

– Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (t.j. Dz.U. z 2019 r. poz. 1781) w brzmieniu obowiązującym w kontrolowanym okresie,

– Zarządzenie Ministra Finansów, Funduszy i Polityki Regionalnej z dnia 29 grudnia 2020 r. w sprawie wprowadzenia Polityki Ochrony Danych Osobowych (Dz. U. MFFiPR z 2020 r. poz. 37),

– Zarządzenie Ministra Finansów z dnia 10 marca 2022 r. w sprawie Systemu Zarządzania Bezpieczeństwem Informacji i Polityki Bezpieczeństwa Informacji Resortu Finansów (Dz. Urz. MF z 2022 r. poz. 19), zmienione następnie Zarządzeniem Ministra Finansów z dnia 25 lipca 2022 r. zmieniającym zarządzenie w sprawie Systemu Zarządzania Bezpieczeństwem Informacji i Polityki Bezpieczeństwa Informacji Resortu Finansów (Dz. Urz. MF z 2022 r. poz. 80),

– Zarządzenie 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),

- 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 (utraciło moc w związku z wejściem w życie 17 października 2025 r. Zarządzenia Nr 146/2025),
- Zarządzenie Nr 146/2025 Dyrektora Izby Administracji Skarbowej w Poznaniu z dnia 17 października 2025 r. w sprawie Systemu Zarządzania Bezpieczeństwem Informacji i polityk bezpieczeństwa w Izbie Administracji Skarbowej w Poznaniu,
- Komunikaty na stronie intranetowej Izby Administracji Skarbowej w Poznaniu, pisma do komórek organizacyjnych oraz maile zobowiązujące wszystkich pracowników do zapoznania się z komunikatem "Nadużywanie nadanych uprawnień w systemach Informatycznych" a także przypominające o treści §24 Polityki Bezpieczeństwa Informacji Resortu Finansów (PBI RF), tj.
  - naruszenie bezpieczeństwa informacji może być uznane za ciężkie naruszenie obowiązków pracowniczych,
  - 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.

Kontrolą objęto łącznie 11 pracowników zatrudnionych w komórkach SKA (6), SOB (1), SPO (1), SKI (2), SER (1).

Inspektor Ochrony Danych oraz Zespół Inspektora Ochrony Danych w Izbie Administracji Skarbowej w Poznaniu

Dyrektor Izby Administracji Skarbowej w Poznaniu powołał Inspektora Ochrony Danych oraz - decyzją (…) w sprawie wyznaczenia w Izbie Administracji Skarbowej w Poznaniu składu Zespołu Inspektora Ochrony Danych - wyznaczył skład osobowy Zespołu Inspektora Ochrony Danych w Izbie Administracji Skarbowej w Poznaniu.

Obowiązkowe szkolenia

Szkolenia okresowe z zakresu ochrony informacji prawnie chronionych zgodnie z § 24 ust. 5 (…) 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).

Obligatoryjne szkolenia dla pracowników:

- RODO Unijne rozporządzenie o ochronie danych osobowych (Atena-3),
- Bezpieczeństwo teleinformatyczne w resorcie finansów (Atena 3),
- Bezpieczeństwo informacji w Resorcie Finansów – wybrane zagadnienia (Atena-3),
- Bezpieczeństwo teleinformatyczne – szkolenie dedykowane dla pracowników resortu finansów.

Według danych udostępnionych przez Pierwszy Dział Personalny (IPP1) ustalono, że pracownicy objęci próbą, ukończyli nw. szkolenia w wymaganych terminach.

- RODO Unijne rozporządzenie o ochronie danych osobowych,
- Bezpieczeństwo informacji w Resorcie Finansów – wybrane zagadnienia (Atena-3),
- Bezpieczeństwo teleinformatyczne – szkolenie dedykowane dla pracowników resortu finansów.

Szkolenie „Bezpieczeństwo teleinformatyczne w resorcie finansów" (Atena3) należało ukończyć do 15 maja 2024 r. Pracownik (…) nie ukończyła szkolenia.

Naczelnik Urzędu wyjaśnił, że ww. pracownik przebywał na urlopie macierzyńskim do dnia 14 lipca 2024 r. W trakcie trwania kontroli instytucjonalnej zapis na szkolenie został potwierdzony.

Pozostali pracownicy objęci próbą ukończyli szkolenie w ww. terminie.

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, stosownie do § 14 pkt 6 Załącznika do aktu, pracownicy zobowiązani zostali do zapoznania się z zasadami określonymi w wyżej wymienionej Polityce oraz potwierdzenia wykonania tego obowiązku w stosownym oświadczeniu (pismo DIAS w Poznaniu z 18 stycznia 2021 r. nr (…).

W badanej próbie kontrolnej 1 pracownik (…) nie podpisał oświadczenia o zapoznaniu się z zasadami określonymi w Polityce Bezpieczeństwa Danych Osobowych wprowadzonej Zarządzeniem Ministra Finansów, Funduszy i Polityki Regionalnej z dnia 29 grudnia 2020 r.), co stanowi uchybienie.

Wyjaśnienia w tej sprawie złożył Naczelnik, informując, że Pani (…), 28 stycznia 2021 roku zapoznała się, za pośrednictwem SZD, z pismem nr (…) UNP: (…) wraz z załącznikami, tj. Polityką Ochrony Danych Osobowych w resorcie finansów. Na potwierdzenie powyższego przedłożono skany z SZD. Oświadczenie uzupełniono w późniejszym terminie (w trakcie kontroli).

Upoważnienie do przetwarzania danych osobowych

Wszyscy kontrolowani pracownicy (11 osób) posiadali w kontrolowanym okresie aktualne upoważnienia do przetwarzania danych osobowych, które zostały potwierdzone.

Sprawozdanie z przeglądu ochrony danych osobowych

W kontrolowanym okresie od 1 stycznia 2025 r. do 31 grudnia 2025 r. Wieloosobowe Stanowisko Ochrony Danych nie prowadziło sprawdzeń w zakresie przestrzegania przepisów o ochronie danych osobowych w Urzędzie Skarbowym w Pleszewie.

II. Uprawnienia do systemów informatycznych, w tym ewidencjonowanie uprawnień

W celu umożliwienia kompleksowego zarządzania upoważnieniami i uprawnieniami do wybranych systemów informatycznych wdrożono System Zarządzania Upoważnieniami i Uprawnieniami (…), który stanowi scentralizowaną ewidencję upoważnień i uprawnień.

Wspiera zarządzanie ryzykiem w obszarze cyberbezpieczeństwa w kontekście polityki kontroli dostępu i zarządzania aktywami oraz przyczynia się do wsparcia i wzmocnienia nadzoru w obszarze Systemu Zarządzania Bezpieczeństwem Informacji - SZBI

Badanie przeprowadzono na podstawie raportu (…) z (…) oraz raportów z (…) (…).

Zbadano uprawnienia nadane 11 pracownikom Urzędu Skarbowego w Pleszewie.

Aktualnie uprawnienia do systemu informatycznego (…)w Urzędzie Skarbowym w Pleszewie nadawane są z wykorzystaniem (…) –(…). W zakresie pozostałych uprawnień do realizacji procesu zarządzania uprawnieniami do systemów informatycznych wykorzystywany jest system(…)[1].

W kontrolowanym okresie pracownicy komórek SKA (6), SOB (1), SPO (1), SKI (2), SER (1) posiadali dostęp do systemu (…) w US w Pleszewie a także w ramach uprawnień nadawanych przez CSU do (…) – dostęp podstawowy; dostęp rozszerzony posiada 1 pracownik z komórki (…) Pani (…). Pracownicy posiadali także dostępy do innych systemów wykorzystywanych w pracy m.in.(…), (…), (…), (…), (…), (…), (…), (…), (…), (…), (…) i innych.

Badanie przeprowadzono według stanu na 14 kwietnia 2026 r. Zasadniczo nadane uprawnienia odpowiadały zakresowi czynności realizowanemu przez pracowników. Ponadto zgodnie z zaleceniami MF wszyscy pracownicy powinni mieć nadany dostęp do systemu (…). W badanej próbie 3 pracowników nie posiada dostępu do aplikacji: (…), (…), (…). Dostęp do aplikacji (…) umożliwia dostęp do kompleksowej bazy materiałów informacyjnych na temat podatków i cła, w której gromadzone są materiały zawierające aktualne stanowisko resortu finansów dotyczące interpretacji i stosowania przepisów prawa podatkowego i celnego.

W przypadku posiadanych uprawnień w aplikacji (…), zwrócono się do NUS w Pleszewie o uzasadnienie do nadanych uprawnień (kontr) pracownikowi komórki (…) – Panu (…) i (KKCS) Pani (…) – pracownikowi komórki (…).

W odpowiedzi udzielonej przez Naczelnika uprawnienia w tym zakresie są niezbędne z uwagi na fakt, że Pan (…) posiada upoważnienia do prowadzenia nabyć sprawdzających. Zarówno, w 2025 r., jak i w 2026 r. był zaangażowany jako członek zespołu do przeprowadzenia nabyć sprawdzających. Uprawnienie KONTR zostało nadane w związku z wykonywaniem powyższych zadań.

Pani (…) miała nadane uprawnienie KKCS, w związku z koniecznością wprowadzania w systemie (…) czynności sprawdzających, w zakresie weryfikacji miejsca prowadzenia

[1] (…)

działalności gospodarczej (oględziny). Powyższe zadanie realizowane jest obecnie z poziomu (…), natomiast uprawnienia pozostały, ponieważ planuje się przeprowadzanie czynności sprawdzających w komórce SKI w zakresie weryfikacji spełnienia przez podatnika warunków do opodatkowania tzw. CIT-em Estońskim (obecnie odbywa się to na zasadzie oświadczenia składanego przed rejestracją przez podatnika, a w celu większego sformalizowania powyższej czynności planuje się wprowadzenie czynności sprawdzających w tym zakresie).

Uwzględniono powyższe wyjaśnienia.

W zakresie systemu (…) (1 pracownik z próby – (…) ma nadane uprawnienia do rejestrowania i stornowania dokumentu (…) i (…). Aktualnie poza uprawnieniami (…) i (…) pozostałe nadane uprawnienia umożliwiają jedynie przeglądanie danych.

Wśród pracowników objętych próbą w komórce (…) jedna osoba nie posiada dostępu do aplikacji (…). Szczegółowy zakres obowiązków pracownika (…) nie różni się od zakresów obowiązków innych pracowników tej komórki, którzy – z uwagi na wykonywane zadania – posiadają dostęp do wskazanej aplikacji.

Zwrócono się do Naczelnika jednostki z zapytaniem o wskazanie przyczyn braku uprawnień dla pracownika (…) w systemie (…), wraz z prośbą o uzasadnienie nadania jej roli (…) (przeglądanie na poziomie centralnym w aplikacji (…).

Naczelnik wyjaśnił, że pracownik (…) Pani (…) posiada uprawnienia do systemu (…). Nie odzwierciedlono ich w (…). W toku kontroli uzupełniono braki i uaktualniono zapisy w (…) w tym zakresie dla pracownika (…).

Wyjaśnienia Naczelnika potwierdzają, że rola (…) - rola centralna w systemie (…) została nadana Pani (…) w lipcu 2023 r. Nadanie uprawnień miało miejsce w okresie łączenia komórki (…) z komórką (…). Ówczesna pełniąca obowiązki kierownika (…) przyznała Pani (…) dostęp do systemu (…), wzorując się na zakresie uprawnień wcześniej posiadanych przez pracowników komórki (…). Obecnie złożono wniosek o odebranie Pani (…) wskazanego uprawnienia. Nadanie powyższych uprawnień stanowi uchybienie.

Zgodnie z (…), stanowiącą załącznik nr 1 do (…), pkt 6 ppkt 4, blokada dostępu do systemu następuje z chwilą przekazania przez kierującego komórką organizacyjną wniosku, w przypadku długotrwałej (dłuższej niż 3 miesiące) absencji użytkownika.

Pracownik (…), na podstawie wykazu uprawnień użytkownika w aplikacjach, posiada dostęp do systemów (…) oraz (…). Nieobecna jest od 13 listopada 2025 roku.

Do wyżej poruszonej kwestii ustosunkował się Naczelnik wraz z pracownikiem Panem (…), którzy wyjaśnili, że 3 grudnia 2025 roku został złożony wniosek nr (…) dotyczący odebrania Pani (…) uprawnień do wskazanych systemów.

Wniosek został przekazany zgodnie z właściwością do administratora systemu (…), natomiast zgłoszenie dotyczące systemu (…) zostało przekazane do (…). Z uzyskanych informacji wynika, że czynności związane z odebraniem uprawnień w systemie (…) zostały zrealizowane w dniu 10 lutego 2026 roku.

Składający wyjaśnienia wskazali jednocześnie, że po stronie administratora systemów proces realizacji wniosku został zakończony skutecznym odebraniem uprawnień wynikających ze złożonego wniosku z 3 grudnia 2025 roku. Brak wcześniejszego zamknięcia sprawy wynikał z przedłużającego się procesu realizacji zgłoszenia dotyczącego systemu (…).

Pan (…) dodatkowo wyjaśnił, że 4 maja 2026 roku, po zapoznaniu się z przesłanym zapytaniem oraz ponownej analizie dokumentacji, odczytał informację z 28 stycznia 2026 roku dotyczącą konieczności złożenia odrębnego wniosku o odebranie uprawnień do systemu (…). W związku z powyższym, celem ostatecznego uporządkowania sprawy 4 maja 2026 roku dokonał stosownych czynności bezpośrednio w systemie (…) i przedłożył na tę okoliczność stosowne dokumenty.

Złożone wyjaśnienia zostały uwzględnione w części, jednakże stwierdzono niezgodność w zakresie czasu realizacji z obowiązującą procedurą. Zgodnie z jej postanowieniami, blokada dostępu do systemu powinna nastąpić z chwilą przekazania przez kierującego komórką organizacyjną stosownego wniosku, w przypadku długotrwałej (przekraczającej 3 miesiące) nieobecności użytkownika.

Wobec powyższego należy uznać, iż zaistniała sytuacja stanowi uchybienie obowiązującym regulacjom.

W wyniku analizy przeglądania danych w systemach stwierdzono brak logów do systemu (…) u pracowników Pani (…) i Pani (…) w okresie od 1 stycznia 2025 r. do 31 grudnia 2025 r., w wyniku czego Naczelnik poinformował, iż wystąpił o odebranie uprawnień.

Nie stwierdzono, aby wskazane powyżej uchybienia wywołały negatywne skutki dla kontrolowanej jednostki. Należy podkreślić, że w części przypadków NUS, w trakcie trwania kontroli instytucjonalnej oraz w ramach składanych wyjaśnień, usunął część stwierdzonych błędów, dokonał 24 kwietnia 2026 r. pogłębioną analizę uprawnień i złożył wnioski o odebranie konkretnych uprawnień posiadanych przez pracowników, co zostało ocenione pozytywnie.

III. Wykorzystanie systemów informatycznych do celów służbowych

Na podstawie art. 35 ust. 1 pkt 1 ustawy z dnia 16 listopada 2016 r. o Krajowej Administracji Skarbowej (t.j. Dz. U. z 2025 r., poz. 1131 ze zm.), w brzmieniu obowiązującym w kontrolowanym okresie, dalej „ustawa o KAS", organy KAS wykonują swoje zadania przy wykorzystaniu (…).

Przez (…) 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.

Zgodnie z art. 45 ust. 1 ustawy o KAS, 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 potrzeby koniecznej – pracownicy mają zapewniony dostęp tylko do środków przetwarzania informacji (urządzeń teleinformatycznych, systemów, aplikacji, pomieszczeń), które są im konieczne do wykonania powierzonych im zadań,
- Zasada wiedzy koniecznej – pracownicy posiadają dostęp tylko do tych informacji, które są konieczne do realizacji powierzonych im zadań (różne zadania oznaczają różną wiedzę konieczną do ich wykonania, a tym samym inny profil dostępu),
- Zasada indywidualnej odpowiedzialności – za utrzymanie odpowiedniego poziomu bezpieczeństwa poszczególnych aktywów lub ich elementów odpowiadają konkretne osoby, w zakresie nałożonych obowiązków i nadanych uprawnień. Zasada ta dotyczy np. powierzonego sprzętu – każdy pracownik odpowiada za powierzony mu do użytkowania sprzęt komputerowy, wydruków z systemu centralnego wydruku – każdy pracownik odpowiada za sporządzony przez siebie wydruk,
- Zasada zgodności z prawem (zasady przetwarzania 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.

Kontroli poddano przeglądanie danych w systemach: (…), (…) i (…) przez 11 pracowników Urzędu Skarbowego w Pleszewie.

1. (…)

jest głównym systemem w urzędach skarbowych przeznaczonym do obsługi podatków, z wyłączeniem podatków PCC, SD i KP.

System (…) stanowi scentralizowaną bazę danych systemu (…) i systemów okołopoltaxowych:

- (…)
- (…)
- (…)
- (…)
- (…)

Dane w systemie pochodzą ze źródeł elektronicznych (integracja z systemem e- Deklaracja, systemem e-PIT) oraz tradycyjnych dokumentów papierowych składanych przez płatników lub podatników.

System umożliwia obsługę formularzy podatkowych deklaracji, wniosków, decyzji i dokumentów wewnętrznych przygotowanych przez Ministerstwo Finansów. W badanej próbie na 23 przypadki przeglądania danych (NIP/PESEL), związek z prowadzonymi czynnościami służbowymi wykazano w 19, dokumentując związek przeglądania danych z realizowanymi czynnościami służbowymi.

W 4 przypadkach nie udokumentowano, że logowania dotyczące wskazanych numerów PESEL/NIP pozostawały w związku z wykonywaniem czynności służbowych (realizowaną sprawą). W 2 z nich, ze względu na specyfikę wykonywanych przez pracownika Urzędu obowiązków służbowych (pracownik SOB zajmujący się bieżącą obsługą klientów na sali obsługi), przyjęto, że przetwarzanie danych mogło mieć charakter służbowy. W pozostałych 2 stwierdzono brak powiązania przeglądań z realizacją zadań służbowych.

1. Pracownik (…)

nie wykazał, że przeglądanie danych miało związek z czynnościami służbowymi (realizowaną sprawą). Wyjaśnił, że brak możliwości przypisania do konkretnej sprawy.

(…)	(…)	(…)	(…)	(…)	2025-01-29 14:17:19
(…)	(…)	(…)	(…)	(…)	2025-01-29 14:17:23

W związku z powyższym, z uwagi na brak powiązania logowania z konkretną sprawą lub czynnością służbową, przedmiotową sytuację zakwalifikowano jako naruszenie zasady wiedzy koniecznej. W badanym przypadku istnieje ponadto prawdopodobieństwo bezprawnego przetwarzania danych osobowych, tj. z naruszeniem rozporządzenia RODO (zob. przepisy kształtujące zasady przetwarzania danych osobowych - art. 5 rozporządzenia i regulacje dotyczące zgodności przetwarzania z prawem - art. 6 rozporządzenia).

2. Pracownik (…)

potwierdził logowanie w celach prywatnych – przeglądanie swoich danych PESEL (…) wyjaśniając, że firma (…) zmieniła charakter zawartej przez nią umowy - chodzi o lokatę

środków pieniężnych na przełomie roku i chciała sprawdzić, czy za 2024 r. jest PIT-8C i czy będzie obowiązana za ten rok złożyć PIT-38 (do dnia dzisiejszego nie dostała papierowo tej informacji z (…). Poinformowała także, że zdaje sobie sprawę iż jej działanie było niewłaściwe.

(…)	(…)	(…)	(…)	(…)	2025-01-14 12:45:32
(…)	(…)	(…)	(…)	(…)	2025-02-27 11:42:02

Pracownik złożył wyjaśnienia wskazujące, iż zdarzenie miało charakter prywatny i nie pozostawało w związku z realizacją obowiązków służbowych. Przeglądanie danych, jako niezwiązane z realizacją zadań służbowych, stanowi naruszenie zasady wiedzy koniecznej.

Wykorzystanie systemu (…)– w 19 z 23 ocenionych przypadków (82,6%) przeglądanie danych znajdowało odzwierciedlenie w realizowanych czynnościach służbowych. W 2 przypadkach nie można wykluczyć, że przetwarzanie danych osobowych służyło realizacji zadań służbowych (dot. przeglądów przez pracownika SOB). W 2 przypadkach, w których nie wykazano związku przeglądania danych z wykonywanymi czynnościami służbowymi, stwierdzono naruszenie zasady wiedzy koniecznej poprzez wykorzystanie systemu (…) niezgodnie z jego przeznaczeniem (przeglądanie danych niezwiązane z zadaniami służbowymi).

2. (…)

Aplikacja (…) umożliwia między innymi:

- księgowanie przypisów, odpisów, wpłat, zwrotów i zaliczeń nadpłat z tytułu podatków i niepodatkowych należności budżetowych,
- kontrolę terminowej wpłaty należności przez podatników,
- terminowe podejmowanie czynności zmierzających do zastosowania środków egzekucyjnych,
- zaliczanie i zwrot nadpłat,
- rozliczanie i przekazywanie wpływów poszczególnym budżetom i innym wierzycielom, sporządzanie sprawozdań,
- wydawanie zaświadczeń o wysokości zaległości podatkowych.

Ocenie poddano 21 przypadków przeglądania danych. Spośród nich w 13 przypadkach wykazano związek z prowadzonymi czynnościami służbowymi, dokumentując wykorzystanie systemu (…) do realizacji zadań służbowych. W odniesieniu do logowań pozostających w związku z wykonywanymi czynnościami służbowymi, m.in. dotyczącymi realizacji wniosków o wydanie zaświadczenia o niezaleganiu lub wezwań do złożenia wniosku o stwierdzenie nadpłaty, przedłożono dokumenty źródłowe potwierdzające zasadność dostępu do systemu.

W 2 przypadkach, ze względu na specyfikę wykonywanych przez pracownika Urzędu obowiązków służbowych (pracownik SOB zajmujący się bieżącą obsługą klientów na sali obsługi), dla celów kontroli przyjęto, że przetwarzanie danych mogło mieć charakter służbowy. Niemniej jednak pożądane byłoby dokumentowanie przyczyny logowania do systemów w przypadkach, gdy czynność ta nie jest bezpośrednio związana z prowadzoną

sprawą.

Natomiast w 6 przypadkach stwierdzono brak związku przeglądania danych z wykonywanymi czynnościami służbowymi (realizowanymi sprawami). W tych przypadkach pracownicy Urzędu złożyli następujące wyjaśnienia.

1. Pracownik (…)

(…)	18.07.2025 11:23:28	P_DAN_OS	(…)	(…)	(…)
(…)	18.07.2025 11:23:28	P_DAN_OS	(…)	(…)	(…)
(…)	18.07.2025 11:23:36	P_DAN_OS	(…)	(…)	(…)
(…)	18.07.2025 11:23:53	P_DAN_OS	(…)	(…)	(…)
(…)	18.07.2025 11:23:56	P_DAN_OS	(…)	(…)	(…)
(…)	18.07.2025 11:23:56	P_DAN_OS	(…)	(…)	(…)
(…)	18.07.2025 11:24:08	P_DAN_OS	(…)	(…)	(…)
(…)	18.07.2025 11:24:13	P_DAN_OS	(…)	(…)	(…)
(…)	18.07.2025 11:24:16	P_DAN_OS	(…)	(…)	(…)
(…)	18.07.2025 11:24:23	P_DAN_OS	(…)	(…)	(…)
(…)	18.07.2025 11:25:41	P_DAN_OS	(…)	(…)	(…)
(…)	18.07.2025 11:25:50	P_DAN_OS	(…)	(…)	(…)

Jako przyczynę przeglądania swoich danych, tj. (…) 18 lipca 2025 r. pomiędzy godziną (11:23-11:25) wskazano sprawdzenie w systemie, czy wyrażono zgodę w e -US na otrzymywanie e-korespondencji.
Ujawnione w toku kontroli przetwarzanie przez pracownika Urzędu danych osobowych, jako niezwiązane z realizacją zadań służbowych, stanowi naruszenie zasady wiedzy koniecznej.
Nie stwierdzono innych logowań pracownika na swoje dane osobowe, lub dane osobowe innych podmiotów, które pozostawałyby bez związku z wykonywanymi zadaniami służbowymi.

2. Pracownik (…) (…) przeglądała swoje dane. Zwrócono się o wyjaśnienia wskazanych logowań.

(…)	18.07.2025 12:44:57	P_DAN_OS	(…)	(…)	(…)
(…)	18.07.2025 12:44:57	P_DAN_OS	(…)	(…)	(…)

Jako przyczynę przeglądania swoich danych, tj. PESEL(…) 18 lipca 2025 r., godzina 12:44 wskazano sprawdzenie, czy skutecznie wyrażono zgodę na e-korespondencję w e- US, ponieważ wystąpiły problemy techniczne podczas próby wyrażenia zgody na e- korespondencję. Powyższe miało miejsce z uwagi na zagrożenie nieosiągnięcia pożądanej wartości miernika przez US w Pleszewie. 4.5.1. Badanie liczby wyrażonych zgód na doręczanie korespondencji za pośrednictwem e-Urzędu Skarbowego.

Odnosząc się do złożonych wyjaśnień, stwierdzono, że wykorzystano dostęp do systemu bez związku z prowadzonymi przez pracowników sprawami. Każdorazowy dostęp do danych musi wynikać z przydzielonej do prowadzenia sprawy służbowej, co nie znajduje potwierdzenia w złożonych wyjaśnieniach. Ujawnione w toku kontroli przetwarzanie przez pracownika Urzędu danych osobowych, jako niezwiązane z realizacją zadań służbowych, stanowi naruszenie zasady wiedzy koniecznej.

Nie zarejestrowano w okresie objętym kontrolą innych logowań o podobnym charakterze, co wskazuje na brak powtarzalności tego typu działań.

3. Pracownik (…)(…), przeglądała swoje dane oraz dane członków rodziny. Zwrócono się o wyjaśnienia wskazanych logowań, tj.

	24.02.2025 07:05:54	P_DAN_OS	(…)	(…)	(…)
	24.02.2025 07:05:55	P_DAN_OS	(…)	(…)	(…)
	24.02.2025 07:06:05	PLTX_DOK	(…)	(…)	(…)
	24.02.2025 07:06:05	PLTX_DOK	(…)	(…)	(…)
	24.02.2025 07:07:22	P_DAN_OS	(…)	(…)	(…)
	24.02.2025 07:07:22	P_DAN_OS	(…)	(…)	(…)
	24.02.2025 07:07:34	PLTX_DOK	(…)	(…)	(…)
	24.02.2025 07:07:34	PLTX_DOK	(…)	(…)	(…)

Wyjaśnienia złożone przez pracownika Panią (…) potwierdzają, że osoby wymienione w tabeli są spokrewnione tj. (…) – mąż, (…) – teść,(…) – teściowa (domownicy). Logowanie na konto członków rodziny było spowodowane weryfikacją wpływu zeznania podatkowego PIT-37 za 2024 roku oraz weryfikacją aktualnego rachunku bankowego.

Wszystkie logowania miały miejsce 24 lutego 2025 r. w godzinach 07:05-07:07, nie zarejestrowano w okresie objętym kontrolą innych logowań o podobnym charakterze, co wskazuje na brak powtarzalności tego typu działań.

Nieakceptowalne jest przeglądanie danych w systemach osób, wobec których pracownik nie prowadzi spraw, w tym danych osób z rodziny.

Powyższe wskazuje na wykorzystanie systemu (…) niezgodnie z przeznaczeniem (przeglądanie danych niezwiązanych z czynnościami służbowymi), co stanowi naruszenie zasady potrzeby koniecznej. W badanym przypadku istnieje ponadto prawdopodobieństwo bezprawnego przetwarzania danych osobowych, tj. z naruszeniem rozporządzenia RODO (zob. przepisy kształtujące zasady przetwarzania danych osobowych - art. 5 rozporządzenia i regulacje dotyczące zgodności przetwarzania z prawem - art. 6 rozporządzenia). Do zdarzenia doszło wskutek świadomego działania pracownika przetwarzającego dane. Nieuprawnione zapoznanie się z danymi osobowymi stanowi nieprawidłowość.

W przypadku pracownika (…) zarejestrowano ponadto przeglądanie danych współpracownika Pana (…) w (…).

W tej sprawie przyjęto wyjaśnienia obu pracowników, zarówno Pani (…) i Pana (…), złożone 10 maja 2026 roku.

Pracownik komórki (…) Pani (…) oświadczyła, że przeglądała w systemie pracownika Pana (…), 4 kwietnia 2025 roku. Powyższa sytuacja miała miejsce na prośbę pracownika Pana (…) w związku z potwierdzeniem dokonania przeksięgowania nadpłaty PIT-37 za 2024 r. na zobowiązanie w podatku PIT-38 za 2024 r. w kwocie 70,00 zł. Wyjaśnienia zostały podpisane przez obu pracowników.

(…)	04.04.2025 13:11:19	P_DAN_OS	(…)	(…)	(…)
(…)	04.04.2025 13:11:20	P_DAN_OS	(…)	(…)	(…)
(…)	04.04.2025 13:11:40	PLTX_DOK	(…)	(…)	(…)

Powyższe wyjaśnienia zostały uwzględnione. Niemniej sprawy podatkowe pracowników Urzędu winny być załatwiane na zasadach i w trybie właściwym dla wszystkich podatników.

Podsumowując wykorzystanie systemu (…) – w 13 z 21 ocenionych przypadków (61,9%) przeglądanie danych znajdowało odzwierciedlenie w realizowanych czynnościach służbowych, w 2 przypadkach nie sposób wykluczyć, że przeglądanie służyło realizacji zadań służbowych dot. przetwarzania danych przez pracownika (…), natomiast w 6 przypadkach (28,6%) nie wykazano związku przeglądania danych z wykonywanymi czynnościami służbowymi (realizowanymi sprawami).

3. (…)

(…) jest to system informatyczny do utrzymywania i przeglądania Centralnego Rejestru Podmiotów, którego integralną częścią jest (…)(…). Zawiera zatem nie tylko dane klientów konkretnego urzędu, ale dane podatników z całego kraju.

Informacje o wszystkich wykonywanych przez operatorów operacjach w aplikacji (…) zapisywane są w bazie danych. Zapisywana jest informacja o każdym wywołaniu akcji, zarówno wykonane poprawne, jak i z błędem. W przypadku, gdy wykonanie akcji nie powiodło się zapisywany jest również kod błędu, który pojawił się na ekranie operatora, celem monitorowania przeprowadzanych przez poszczególnych pracowników zadań i oceny ich pracy.

Taki sposób monitorowania powinien kształtować świadomość użytkowników, że dostęp do systemu oraz przetwarzanych w nim danych jest dopuszczalny wyłącznie w zakresie wynikającym z powierzonych im obowiązków służbowych i w związku z prowadzonymi sprawami. Wyklucza to wykorzystywanie systemu do przeglądania danych bez uzasadnionego celu służbowego.

W badanej próbie na 32 przeglądania danych, bezpośredni związek z prowadzonymi czynnościami służbowymi wykazano w 28 przypadkach, przedkładając stosowną dokumentację potwierdzającą zasadność dostępu do danych.

W 4 przypadkach nie wykazano, że logowania miały związek z czynnościami służbowymi (realizowaną sprawą) - wyjaśniono:

- Pracownik (…)(…) udokumentował logowanie w stosunku do 4 podmiotów.

W przypadku pozostałych trzech, tj. NIP (…), NIP (…), NIP (…),

(…)	13.08.2025 15:07
(…)	13.08.2025 15:03
(…)	13.08.2025 15:07

złożył wyjaśnienia o następującej treści: „różnorodność wykonywanych zadań nie pozwala na przypisanie do konkretnej sprawy. Prawdopodobnie zadanie akcyjne. W tym czasie przeglądano większą ilość podatników”.

2 lipca 2026 r. pracownik złożył dodatkowe wyjaśnienia i przedstawił następujące fakty:

- wskazane podmioty podlegają pod właściwość Naczelnika Pierwszego Urzędu Skarbowego w Kaliszu,

- wszystkie wskazane podmioty prowadzą działalność gospodarczą w zakresie transportu drogowego towarów,
- większość tych podmiotów wskazuje adres siedziby działalności gospodarczej jako blok mieszkalny.

Pracownik (…) wyjaśnił także, że przegląd danych w systemie (…) miał miejsce 13 sierpnia 2025 r. po godz. 15: „ten dzień szczegółowo zapadł w mojej pamięci, gdyż miałam wizytę „ciężkiego" podatnika, z uwagi na sezon urlopowy zastępowałam kierownika działu oraz musiałam wyjść służbowo w celu realizacji zadania w ramach akcji LATO2025 (przeprowadzenie nabyć sprawdzających). Do siedziby urzędu powróciłam o godz. 14:10 a pracę zakończyłam o godz. 15:16. Pomimo tak pamiętnego dnia w chwili obecnej, po upływie blisko roku od wyżej wskazanej daty, nie jestem w stanie przyporządkować wskazanych logowań do konkretnej sprawy, ale mogę zapewnić, że były one powiązane z prowadzoną w urzędzie sprawą. Nie jestem osobą, która bezpodstawnie sprawdza podmioty w bazie danych urzędu skarbowego. Doskonale znam konsekwencje wykorzystywania danych do celów prywatnych".

Ponadto pracownik złożył oświadczenie do kontroli instytucjonalnej: „Oświadczam, że pomiędzy mną a podmiotami przeglądającymi nie istnieją żadne powiązania, tj. nie posiadam z tymi podmiotami żadnych powiązań rodzinnych, koleżeńskich, sąsiedzkich lub jakichkolwiek innych".

Należy wskazać, iż wykonywane czynności, w tym zadania o charakterze akcyjnym, powinny znajdować odzwierciedlenie w prowadzonej dokumentacji służbowej, w szczególności w raportach, adnotacjach, rejestrach lub innych materiałach potwierdzających ich realizację. Brak stosownej dokumentacji uniemożliwia jednoznaczne potwierdzenie charakteru podejmowanych czynności oraz powoduje powstanie wątpliwości, czy wszystkie przypadki logowań do systemów miały wyłącznie charakter służbowy i pozostawały w bezpośrednim związku z realizacją powierzonych obowiązków. Niemniej jednak złożone w toku kontroli wyjaśnienia wskazują, że nie można wykluczyć, iż przetwarzanie danych osobowych służyło realizacji zadań służbowych. Okoliczność ta nie eliminuje jednak uchybienia polegającego na braku udokumentowania wykonywanych czynności, który uniemożliwia wykazanie związku poszczególnych przypadków dostępu do danych osobowych z realizacją konkretnych obowiązków służbowych, a tym samym zapewnienie rozliczalności procesu przetwarzania danych osobowych.

- Pracownik (…)(…) udokumentował logowanie w stosunku do 2 podmiotów.

W 1 przypadku, NIP: (…)

(…)	10.09.2025 14:08

złożył natomiast wyjaśnienia o następującej treści: „nie ma jego wystąpienia w lokalnej bazie dlatego weryfikowałam go w (…). Do tej pory nie prowadziłam żadnych rejestrów, na podstawie których mogłabym sprawdzić na potrzeby jakiej sprawy i kto zwrócił się do (…) o sprawdzenie właściwości urzędu lub potwierdzenie istnienia takiej osoby. Do komórki

rejestracji (pomimo posiadania uprawnień do przeglądania danych) zwraca się większość pracowników, którzy często chcą sprawdzić lub się upewnić czy poprawnie dokonali sprawdzenia. Ponadto, codziennie opisuję obiegówki, na podstawie których komórka (…) udziela informacji uprawnionym podmiotom (KCIK, SĄD, ZUS, PROKURATURY) niejednokrotnie w jednym piśmie jest zapytanie o kilka osób, natomiast w temacie zakładanej sprawy nie są wszystkie osoby wymienione i trudno jest mi w tej chwili odnaleźć dokument na podstawie, którego sprawdzałam wystąpienie. Często sprawdzamy wystąpienia podmiotów do czynności majątkowych, do czynności sprawdzających SKA (weryfikowanie poprawności odliczenia ulgi rodzinnej przez obojga małżonków, w większości jeden z małżonków podlegał pod inny urząd)".

Ponadto pracownik złożył oświadczenie do kontroli instytucjonalnej: „Oświadczam, że pomiędzy mną a podmiotem/podmiotami przeglądającymi nie istnieją żadne powiązania, tj. nie posiadam z tymi podmiotami żadnych powiązań rodzinnych, koleżeńskich, sąsiedzkich lub jakichkolwiek innych".

W toku przeprowadzonych czynności kontrolnych nie potwierdzono, aby przeglądanie danych pozostawało w bezpośrednim związku z realizacją zleconych zadań służbowych. W związku z powyższym, z uwagi na brak powiązania logowania z konkretną sprawą lub czynnością służbową, badane zdarzenia zakwalifikowano jako naruszenie zasady wiedzy koniecznej. W badanym przypadku istnieje ponadto prawdopodobieństwo bezprawnego przetwarzania danych osobowych, tj. z naruszeniem rozporządzenia RODO (zob. przepisy kształtujące zasady przetwarzania danych osobowych - art. 5 rozporządzenia i regulacje dotyczące zgodności przetwarzania z prawem - art. 6 rozporządzenia).

Na podstawie badanej próby kontrolnej stwierdzono, że:

- wykorzystanie systemu (…) – w 82,6% przypadków przeglądania danych znajdowało odzwierciedlenie w realizowanych czynnościach służbowych,
- wykorzystanie systemu (…) – w 61,9% przypadków przeglądania danych znajdowało odzwierciedlenie w realizowanych czynnościach służbowych,
- wykorzystanie systemu (…) – w ponad 87,5% przypadków przeglądania danych znajdowało odzwierciedlenie w realizowanych czynnościach służbowych.

Mając na uwadze zakres, różnorodność i złożoność zadań realizowanych przez wytypowanych do próby pracowników w większości przypadków uzasadnione było korzystanie z badanych systemów informatycznych w celu realizacji obowiązków służbowych.

Jednocześnie stwierdzony udział przypadków, dla których nie wykazano związku z wykonywanymi czynnościami służbowymi (wszystkie badane systemy informatyczne), wskazuje na konieczność dalszego wzmacniania mechanizmów nadzoru nad zasadnością dostępu do danych oraz monitorowania wykorzystania systemów informatycznych.

Kontrola Funkcjonalna

W kontrolowanym okresie kontrole funkcjonalne powinny być realizowane zgodnie

z Procedurą kontroli funkcjonalnej wprowadzoną przez Dyrektora Izby Administracji Skarbowej w Poznaniu Zarządzeniem nr (…) z dnia (…) w sprawie wprowadzenia kontroli funkcjonalnej, następnie zmienioną zarządzeniem nr (…), (…), (…) i nr (…)

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 z wyjątkiem jednej sprawy, na której nie uwidoczniono numeru.

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.

Kierownicy komórek oraz Naczelnik Urzędu Skarbowego prowadzili kontrole funkcjonalne obejmujące swoim zakresem kwestie aktualności i zasadności nadawania uprawnień do systemów informatycznych, ujmując temat w Planie kontroli funkcjonalnej na 2025 r. ”Zasadność udzielania dostępu do systemów inf. oraz zakresu tego dostępu”.

Przeprowadzone kontrole dokumentowano w Informacjach o przeprowadzonej kontroli funkcjonalnej. W wyniku kontroli funkcjonalnych nie stwierdzono nieprawidłowości.

Kontrolujący **(stanowisko służbowe Imię, nazwisko)**	**Okres kontroli**	**Data przeprowadzenia**	**Nr w SZD**	**Zalecenia pokontrolne**
(…)	12.10.2025 r.	12.10.2025 r.	(…)	brak
(…)	01.12.2025 r.- -29.12.2025 r.	29.12.2025 r.	(…)	brak
(…) Naczelnik Urzędu	01.01.2025 r.- -30.09.2025 r.	01.01.2025 r. - 31.10.2025 r.	(…)	brak
(…) (…)	01.01.2025 r.- -30.06.2025 r. 01.07.2025 r.- -31.12.2025 r.	01.07.2025 r. 17.12.2025 r.	(…) (…)	brak brak
(…)	Stan na dzień 01.09.2025 r.	01.09.2025 r.	(…) (…) (…) (…) (…) (…) (…) (…)	brak

			(…)(…)	
(…)	01.01.2025- -14.10.2025	14.10.2025 r.	(…)	brak
(…)	01.01.2025- -27.10.2025	27.10.2025 r.	-	brak

Zapisy zawarte w informacjach o przeprowadzonej kontroli funkcjonalnej zostały sformułowane w sposób ogólny. Brakuje materiałów źródłowych potwierdzających przeprowadzenie kontroli, takich jak raporty, wykazy lub inne dokumenty.

W komórce (…) nie wskazano, których pracowników objęto weryfikacją.

W komórce (…) nie wskazano systemów informatycznych, w których kontrolowano zgodność i zasadność posiadanych przez pracowników uprawnień dostępu.

W zakresie realizacji procesu zarządzania uprawnieniami do systemów informatycznych konieczne jest przeprowadzanie kontroli (co najmniej raz na pół roku) przez kierujących komórkami w zakresie przydzielania uprawnień do systemów informatycznych i nadanych upoważnień. Powyższe wynika z § 10 ust. 2 Zarządzenia (…) Dyrektora Izby Administracji Skarbowej w Poznaniu z 28 września 2018 r. w sprawie wykorzystania systemu (…) do realizacji procesu zarządzania uprawnieniami do systemów informatycznych funkcjonujących w Izbie Administracji Skarbowej w Poznaniu i podległych urzędach, zmienione Zarządzeniem (…) Dyrektora Izby Administracji Skarbowej w Poznaniu z dnia (…).

Kontrola w zakresie zgodności i zasadności dostępu (uprawnień pracowników do systemów informatycznych w świetle wykonywanych zadań) została przeprowadzona w komórce (…) Z przekazanych materiałów wynika, że Naczelnik Urzędu weryfikował zasadność udzielania pracownikom dostępu do systemów informatycznych, w wyniku których nie miał uwag.

W wyniku analizy zasadności udzielania dostępu do systemów informatycznych w ramach kontroli instytucjonalnej stwierdzono uchybienia w przedmiotowym zakresie, m.in. posiadanie przez pracowników nadmiarowych uprawnień. Rozbieżności pomiędzy wynikami kontroli funkcjonalnej przeprowadzonej przez Organ i ustaleniami kontroli instytucjonalnej mogą świadczyć o niewystarczającej skuteczności kontroli funkcjonalnej w identyfikowaniu ryzyk w badanym obszarze, a także o braku jej oparcia na rzetelnej i kompleksowej analizie ryzyka. W związku z ujawnionymi w toku kontroli instytucjonalnej nieprawidłowościami (poza ww. nadmiarowym przyznaniem uprawnień do systemów informatycznych, stwierdzono wykorzystanie dostępu do systemów bez związku z realizacją zadań służbowych) zasadne jest dokonanie przeglądu oraz aktualizacji Rejestru Ryzyk w obszarze objętym kontrolą.

W przypadku pracowników posiadających nadmiarowe uprawnienia, proces ich aktualizacji został rozpoczęty w trakcie czynności kontrolnych, co należy ocenić jako właściwą reakcję Naczelnika Urzędu na zapytania kierowane w trakcie czynności oraz potwierdzenie bieżącego podejmowania działań zmierzającego do usunięcia stwierdzonych nieprawidłowości.

W skontrolowanym zakresie stwierdzono następujące nieprawidłowości pkt 1-2

i uchybienia pkt 3-6.

1. Przeglądanie i wykorzystywanie danych w systemach: (…), (…) i (…) bez związku z prowadzoną przez pracownika sprawą służbową, co stanowi naruszenie:

- zasady 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),
- Polityki Bezpieczeństwa Informacji Resortu Finansów,
- Polityki Ochrony Danych Osobowych,
- 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 zgodności z prawem,

a także mogło się wiązać z naruszeniem 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 Nr 119 z 4.05.2016 r., str. 1), w szczególności zasad przetwarzania danych osobowych (art. 5 rozporządzenia) i zgodności przetwarzania z prawem (art. 6 rozporządzenia).

2. Niezłożenie oświadczenia o zapoznaniu się z Polityką Ochrony Danych Osobowych, tj. z Załącznikiem do Zarządzenia Ministra Finansów, Funduszy i Polityki Regionalnej z dnia 29 grudnia 2020 r. w sprawie wprowadzenia Polityki Ochrony Danych Osobowych (Dz.Urz.MFFiPR z 2020 r., poz. 37), co stanowi naruszenie § 14 pkt 6 Polityki.

3. Niedokumentowanie wykonywanych czynności (zadań akcyjnych), skutkujące brakiem możliwości wykazania związku poszczególnych przypadków dostępu do danych osobowych z realizacją konkretnych obowiązków służbowych.

4. Nieukończenie przez pracownika obowiązkowego szkolenia „Bezpieczeństwo teleinformatyczne w resorcie finansów” (Atena3).

5. Posiadanie przez pracowników nadmiarowych uprawnień do systemów informatycznych. Brak rzetelnego przeprowadzenia przeglądu aktualności i zasadności nadanych uprawnień w wymaganych terminach, nie rzadziej niż raz na poł roku.

6. Nie w pełni dochowano zapisów obowiązującej procedury zarządzania uprawnieniami do systemów informatycznych. Zgodnie z jej postanowieniami blokada dostępu do systemu, w tym przypadku Wro-System, powinna nastąpić z chwilą przekazania przez kierującego komórką organizacyjną stosownego wniosku, w przypadku długotrwałej

nieobecności użytkownika przekraczającej 3 miesiące.

Osoby odpowiedzialne za stwierdzone nieprawidłowości:

- w zakresie nieprawidłowości określonej w punkcie 1:
  - (…),
  - (…),
  - (…),
  - (…),
  - (…),
  - (…) do dnia (…) oraz w trybie nadzoru ww. kierownik (…), (…)kierownik (…) do dnia (…) i Naczelnik Urzędu Skarbowego w Pleszewie,
- w zakresie nieprawidłowości określonej w punkcie 2 – (…) oraz w trybie nadzoru ww. kierownik (…) i Naczelnik Urzędu Skarbowego w Pleszewie.

Podsumowując, zagadnienie dotyczące uprawnień do systemów informatycznych i ich wykorzystanie do celów służbowych oceniono pozytywnie z nieprawidłowościami.
Wystąpiło nieuprawnione przeglądanie informacji przez użytkowników systemów informatycznych, które mogło skutkować naruszeniem przepisów RODO. Nadto działania ww. pracowników Urzędu naruszały zasadę rzetelności, o której 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), przepisy prawa wewnętrznego w zakresie bezpieczeństwa informacji, przepisy Polityki Ochrony Danych Osobowych i Polityki Bezpieczeństwa Informacji Resortu Finansów.

Wyjaśnienia wymaga, że także w przypadku korzystania z narzędzi informatycznych przez pracownika SOB nie ustalono w toku kontroli powiązań między przetwarzaniem danych w systemie (…) oraz w systemie (…) i realizowanymi czynnościami służbowymi (pracownik nie potrafił wykazać takiego związku). W tym przypadku, z uwagi na specyfikę realizowanych zadań (bezpośrednia obsługa klientów KAS na sali obsługi) nie wykluczono jednak, że poddane weryfikacji przeglądy służyły celom służbowym. Niemniej stwierdzona w toku kontroli okoliczność braku możliwości dokonania oceny zgodności z prawem działań pracownika ww. komórki Urzędu wskazuje na słabość funkcjonującego w Urzędzie systemu bezpieczeństwa informacji. Zatem - mimo, że w omawianym przypadku nie sformułowano zarzutu nieprawidłowości ani uchybienia - ustalenia kontroli powinny skłonić Naczelnika Urzędu Skarbowego w Pleszewie do wprowadzenia narzędzi, które pozwolą jednoznacznie stwierdzić, czy przetwarzanie danych także przez pracowników (…) nie narusza zasad bezpieczeństwa informacji lub zasad ochrony danych osobowych (np. poprzez

rejestrowanie daty, nazwy systemu i powodu przeglądania, w przypadku, gdy nie jest ono związane z prowadzoną z żadną sprawą służbową prowadzoną w analizowanym okresie).

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.

W zakresie korzystania z systemów informatycznych w Resorcie Finansów obowiązuje reguła indywidualnego konta i uwierzytelniania (identyfikacji i autoryzacji), która zapewnia rozliczalność wszystkich działań wykonywanych przez użytkownika w systemach informatycznych stanowiących własność Resortu Finansów. Zgodnie z § 24 Polityki Bezpieczeństwa Informacji Resortu Finansów, naruszenie bezpieczeństwa informacji może być uznane za ciężkie naruszenie obowiązków pracowniczych a 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.

[dowód: akta kontroli poz. 17-29 w SZD]

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 realizowanymi sprawami służbowymi (przydzieloną do prowadzenia sprawą), a w przypadku próśb lub poleceń innych osób każdorazowo odnotowywać i uzgadniać z przełożonym tak aby zapewnić rozliczalność w zakresie przeglądania danych. Przeprowadzać kontrole funkcjonalne w zakresie wykorzystania nadanych uprawnień w systemach informatycznych przez pracowników. 2. Potwierdzać pisemnie zapoznanie się z wprowadzanymi w życie aktami prawnymi w każdym przypadku, gdy przepis prawa tak stanowi. 3. Dokumentować wykonywanie czynności (zadań akcyjnych). Dokumenty te (np. notatki, rejestry) prowadzić w taki sposób, by możliwe było na ich podstawie wykazanie związku przetwarzania w systemach danych z realizacją obowiązków służbowych. 4. Wzmocnić nadzór nad realizacją obowiązkowych szkoleń przez podległych pracowników i zapewnić ich terminową realizację. 5. Dokonywać - co najmniej raz na pół roku - przeglądu oraz weryfikacji nadanych

uprawnień użytkowników w systemach informatycznych pod kątem ich adekwatności do aktualnie realizowanych obowiązków służbowych.

6. Odbierać uprawnienia do systemów długotrwale nieobecnym pracownikom bez zbędnej zwłoki, w terminach wskazanych w przepisach prawa wewnętrznego (terminowo składać komplet dokumentów/wniosków do odbioru uprawnień do systemów informatycznych).
7. Przeprowadzić kontrolę funkcjonalną w zakresie stwierdzonych nieprawidłowości i uchybień oraz przekazać informację o rezultatach wdrożenia zaleceń pokontrolnych w terminie 9 miesięcy od dnia udzielenia informacji o sposobie wykonania zaleceń pokontrolnych.

Ocena wskazująca na niezasadność zajmowania stanowiska lub pełnienia funkcji przez osobę odpowiedzialną za stwierdzone nieprawidłowości

Pouczenie

Stosownie do przepisu art. 52 ust. 5 ustawy z dnia 15 lipca 2011 r. o kontroli w administracji rządowej (t.j. Dz. U. z 2026 r., poz. 158) Naczelnik Urzędu w terminie 3 dni roboczych od dnia otrzymania sprawozdania z kontroli ma prawo przedstawić do niego stanowisko; nie wstrzymuje to jednak realizacji ustaleń kontroli.

Termin złożenia informacji

W przypadku stwierdzonych uchybień bądź nieprawidłowości w terminie 30 dni od dnia otrzymania sprawozdania z kontroli 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 – Beata Korczowska

2. Z-ca DIAS – Arkadiusz Radziejewski
3. Z-ca DIAS – Robert Stangret
4. Z-ca DIAS – Dariusz Strugliński
5. Z-za DIAS – Agata Wciórka
6. Wieloosobowe Stanowisko Ochrony Danych (IWD)
7. Dział Bezpieczeństwa i Ochrony Informacji oraz Cyberbezpieczeństwa i Zgodności (IWO)