Krajowa Administracja Skarbowa

Izba Administracji Skarbowej
w Gdańsku

2201-IWW[1].0921.33.2023

SPRAWOZDANIE

Z KONTROLI

Izba Administracji Skarbowej w Gdańsku

I. Dane identyfikacyjne kontroli

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

Jednostka kontrolowana:
Pierwszy Urząd Skarbowy w Gdyni
ul. Władysława IV 2/4
81-353 Gdynia

Kierownik jednostki kontrolowanej:
Pani Anna Jankowska - Naczelnik Pierwszego Urzędu Skarbowego w Gdyni (zwany dalej Naczelnikiem lub NUS) powołana na stanowisko Naczelnika od 1.06.2022 roku

Kontrolerzy:
Maria Kubińska - Matciak - starszy ekspert skarbowy– koordynator kontroli,
Wiktor Lipiński – ekspert skarbowy,
działający na podstawie upoważnienia Dyrektora Izby Administracji Skarbowej Nr 2201 - IWW[1]1.0921.33.2023 z 8.11.2023 roku

Data rozpoczęcia czynności kontrolnych: 8.11.2023 roku

Data zakończenia czynności kontrolnych: 28.12.2023 roku

Podstawa prawna prowadzenia kontroli: art. 6 ust. 5 ustawy z dnia 15 lipca 2011 roku o kontroli w administracji rządowej

Wpisano do ewidencji kontroli: poz. 2/2023

Okres objęty kontrolą: od 01.06.2023 roku do 30.09.2023 roku Badaniem zostały objęte również zdarzenia i dokumenty wcześniejsze lub późniejsze, gdy miały związek z przedmiotem kontroli.

Zakres przedmiotowy kontroli: wykorzystanie systemów informatycznych do celów służbowych.

Ocena kontrolowanej działalności

Ocena ogólna:
Działania kierowanego przez Naczelnika Pierwszego Urzędu Skarbowego w Gdyni w badanym zakresie oceniono **negatywnie.**

Uzasadnienie oceny ogólnej:
Wpływ na ocenę ogólną skontrolowanego zakresu miały stwierdzone nieprawidłowości:
1. naruszenie zasady poufności oraz ochrony danych osobowych,

2. naruszenie zasady rozliczalności,
3. nie zrealizowanie polecenia Dyrektora IAS w Gdańsku dotyczącego realizacji w wyznaczonym terminie szkoleń.

Szczegółowe uzasadnienie oceny ogólnej stanowią poniższe ustalenia i uwagi dotyczące kontrolowanych zagadnień.

II. Opis ustalonego stanu faktycznego

Zagadnienie z zakresu badania: *Wykorzystanie systemów informatycznych do celów służbowych.*

Opis stanu faktycznego:

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

- ✓ Regulamin Organizacyjny Pierwszego Urzędu Skarbowego w Gdyni stanowiący załącznik do Zarządzenia nr (…) Dyrektora Izby Administracji Skarbowej w Gdańsku z dnia 31 marca 2023 roku w sprawie nadania Regulaminu Organizacyjnego Pierwszemu Urzędowi Skarbowemu w Gdyni (obowiązujący od 1.04.2023 roku do 30.06.2023 roku);
- ✓ Regulamin Organizacyjny Pierwszego Urzędu Skarbowego w Gdyni stanowiący załącznik do Zarządzenia nr (…) Dyrektora Izby Administracji Skarbowej w Gdańsku z dnia 27 czerwca 2023 roku w sprawie nadania Regulaminu Organizacyjnego Pierwszemu Urzędowi Skarbowemu w Gdyni (obowiązujący od 1.07.2023 roku do nadal);

Zgodnie ze strukturą organizacyjną urzędu Naczelnik sprawuje bezpośredni nadzór nad:

1. Pionem Wsparcia i Obsługi Podatnika (SNUWO):
   - ✓ Działem Wsparcia i Obsługi Bezpośredniej (SWOW),
   - ✓ Referatem Obsługi Bezpośredniej (SOB)
2. Pionem Poboru i Egzekucji (SZNE):
   - ✓ Działem Spraw Wierzycielskich (SEW),
   - ✓ Działem Egzekucji Administracyjnej (SEE),
   - ✓ Działem Rachunkowości (SER),

Zastępca Naczelnika sprawuje bezpośredni nadzór nad:

1. Pionem Orzecznictwa (SZNKP):
   - ✓ Referatem Podatków Dochodowych i Podatku od Towarów i Usług oraz Podatków Majątkowych i Sektorowych (SPV),
2. Pionem Kontroli (SZNK)
   - ✓ Działem Podatków Dochodowych i Podatku od Towarów i Usług oraz Kontroli Podatkowej (SKV),
   - ✓ Referatem Identyfikacji i Rejestracji Podatkowej (SKI),
   - ✓ Pierwszym Referatem Czynności Analitycznych i Sprawdzających (SKA-1),

- ✓ Drugim Działem Czynności Analitycznych i Sprawdzających (SKA-2),
- ✓ Trzecim Działem Czynności Analitycznych i Sprawdzających (SKA-3).

Według Regulaminu organizacyjnego Pierwszego Urzędu Skarbowego w Gdyni, do zadań wszystkich komórek należy wykonywanie zadań w sposób zgodny z prawem, efektywny, oszczędny i terminowy oraz przestrzeganie zasad bezpiecznego przetwarzania informacji. Naczelnik nie wprowadził wewnętrznych procedur dotyczących kontrolowanego obszaru.

W realizacji zadań z zakresu objętego kontrolą obowiązują udokumentowane procedury i uregulowania Dyrektora Izby Administracji Skarbowej w Gdańsku :

- ✓ Polityka Ochrony Danych Osobowych Izby Administracji Skarbowej w Gdańsku stanowiąca załącznik do zarządzenia nr (…) Dyrektora Izby Administracji Skarbowej w Gdańsku z dnia 16 czerwca 2020 roku (obowiązująca do 17.09.2023 roku),
- ✓ Polityka Ochrony Danych Osobowych Izby Administracji Skarbowej w Gdańsku stanowiąca załącznik do zarządzenia nr (…) Dyrektora Izby Administracji Skarbowej w Gdańsku z dnia 18 września 2023 roku,
- ✓ Polityka Bezpieczeństwa Informacji w Izbie Administracji Skarbowej w Gdańsku, wprowadzona zarządzeniem nr (…) DIAS w Gdańsku z dnia 25 maja 2018 roku,
- ✓ Decyzja nr (…) Dyrektora Izby Administracji Skarbowej w Gdańsku z dnia 5 lipca 2022 roku w sprawie wyznaczenia pracowników do spraw bezpieczeństwa danych osobowych w Izbie Administracji Skarbowej w Gdańsku, urzędach skarbowych woj. pomorskiego oraz w Pomorskim Urzędzie Celno-Skarbowym w Gdyni (obowiązująca do 23.07.2023 roku),
- ✓ Decyzja nr (…) Dyrektora Izby Administracji Skarbowej w Gdańsku z dnia 24 lipca 2023 roku w sprawie wyznaczenia pracowników do spraw bezpieczeństwa danych osobowych w Izbie Administracji Skarbowej w Gdańsku, urzędach skarbowych woj. pomorskiego oraz w Pomorskim Urzędzie Celno-Skarbowym w Gdyni,
- ✓ Decyzja nr (…) Dyrektora Izby Administracji Skarbowej w Gdańsku z dnia 22 grudnia 2021 roku w sprawie powołania Zespołu ds. Systemu Zarządzania Bezpieczeństwem Informacji w Izbie Administracji Skarbowej w Gdańsku,
- ✓ Decyzja nr (…) Dyrektora Izby Administracji Skarbowej w Gdańsku z dnia 2 marca 2023 roku w sprawie wyznaczenia merytorycznych aplikacji/systemów informatycznych oraz koordynatorów merytorycznych i ich zastępców.

W kontrolowanym zakresie szczegółowym badaniem objęto wybranych pracowników: Pierwszego Referatu Czynności Analitycznych i Sprawdzających (SKA-1), którym kierowała pani O. N. Podczas nieobecności zastępowała ją pani A. Z.. Zadania komórki realizowało 11 pracowników (łącznie z kierownikiem komórki). Badaniem objęto 2 pracowników, panią D. A. oraz panią W. K..

Do zakresu zadań wykonywanych przez panią D. A. należało:

- analizowanie oświadczeń o stanie majątkowym: wprowadzanie danych z przesłanych oświadczeń majątkowych do Biblioteki Akt, sporządzanie analiz przy wykorzystaniu ANALIZATORA, sprawdzanie poprawności złożonych oświadczeń m.in. poprzez

porównanie danych z oświadczeń majątkowych z danymi z zeznań podatkowych, z informacjami o posiadanych nieruchomościach (CRCM),
- pozyskiwanie i analiza informacji mogących mieć wpływ na powstanie obowiązku podatkowego, w tym o wydatkach i wartości mienia zgromadzonego przez podatnika, analizowanie stanu majątkowego wytypowanych podatników poprzez weryfikację informacji o nich we wszelkich dostępnych aplikacjach i bazach danych.

Do zakresu zadań wykonywanych przez panią W. K. należało:
- prowadzenie czynności sprawdzających w zakresie działania komórki, w szczególności uwzględniających transakcje wewnątrzwspólnotowe w zakresie podatku VAT: weryfikacja danych dostępnych w systemie VIES oraz prowadzenie analiz i czynności sprawdzających w celu wyjaśnienia różnic,
- kontrola i bieżąca analiza informacji podsumowujących VAT-UE i VAT-UEK: analiza informacji oraz wyjaśnianie nieprawidłowości,
- monitorowanie terminowości i wywiązywania się z obowiązku składania informacji i deklaracji podatkowych przez podatników w celu wyegzekwowania realizacji tego obowiązku: analiza raportów i informacji z systemu VIES,
- prowadzenie spraw zmierzających do wykreślenia podatnika z rejestru jako podatnika VAT i VAT-UE w celu aktualizacji bazy czynnych podatników i zapobiegania oszustwom,
- weryfikowanie zgodnie z procedurą wniosków o zwrot podatku od wartości dodanej naliczonego w innym niż Rzeczpospolita Polska państwie członkowskim Wspólnoty Europejskiej składanych przez podatników podatku od towarów i usług w formie elektronicznej na formularzach VAT-REF: analiza wniosków, które wpłynęły do Urzędu w systemie vat-refund.

Zapoznanie pracowników objętych badaniem z Polityką Ochrony Danych Osobowych

Zgodnie z § 14 pkt 6 Polityki Ochrony Danych Osobowych, wprowadzonej Zarządzeniem Ministra Finansów, Funduszy i Polityki Regionalnej z dnia 29 grudnia 2020 roku (dalej: Polityka), każdy pracownik jest zobowiązany do zapoznania się z Polityką i potwierdzenia tego w formie pisemnej. Dyrektor Izby Administracji Skarbowej w Gdańsku pismem nr (…) z 26.01.2021 roku zobowiązał wszystkich pracowników do zapoznania z treścią Polityki za pośrednictwem systemu Qasystent w terminie do 12 lutego 2021 roku i potwierdzenia tego faktu w powyższym systemie.
Pracownicy objęci kontrolą zapoznali się Polityką w systemie Qasystent i potwierdzili ten fakt w dniu 1.02.2021 roku .

Obowiązkowe szkolenia dla pracowników objętych badaniem

Dyrektor Izby Administracji Skarbowej w Gdańsku w pismach kierowanych do Naczelnika Urzędu, polecił wszystkim pracownikom odbyć szkolenia z zakresu:

1) RODO Unijne rozporządzenie o ochronie danych osobowych – dostępne na platformie e-learningowej Atena2, wyznaczony termin: 30.04.2018 roku Szkolenie ukończyła pani W. K., natomiast pani D. A. nie odbyła szkolenia.
2) Bezpieczeństwo teleinformatyczne - dostępne na platformie e-learningowej Atena2, wyznaczony termin: 30.06.2022 roku Szkolenie ukończyła pani W. K. , natomiast Pani D. A. nie ukończyła szkolenia.
3) Naruszenie ochrony danych osobowych – dostępne na platformie e-learningowej Moodle, wyznaczony termin: bezzwłocznie. Pracownicy objęci badaniem ukończyli szkolenie.
4) Zasady bezpieczeństwa informacji - dostępne na platformie e-learningowej Moodle, wyznaczony termin: 13.01.2023 roku Pracownicy objęci badaniem odbyli szkolenie.

Z wyjaśnień NUS z 24.11.2023 roku wynika, że pani D. A. nie zrealizowała szkoleń w wyniku przeoczenia. Szkolenia te odbyła w dniach 16 i 17 listopada 2023.

(Dowód: pismo NUS w SZD, UNP: 2201-23-170943)

Wyjaśnienia nie zmieniają ustaleń kontroli. Brak realizacji w wyznaczonym terminie szkoleń przez panią D. A. dot. RODO Unijne rozporządzenie o ochronie danych osobowych oraz bezpieczeństwo teleinformatyczne stanowi nieprawidłowość, polegającą na nie zrealizowaniu polecenia Dyrektora.

Upoważnienie do przetwarzania danych osobowych

Pracownicy poddani kontroli posiadali w kontrolowanym okresie aktualne upoważnienia do przetwarzania danych osobowych i podpisali stosowne oświadczenie dot. ochrony danych osobowych.

Uprawnienia do systemów informatycznych

Badanie przeprowadzono na podstawie udostępnionych przez Naczelnika wykazu uprawnień i ról z Centralnego Systemu Zarządzania Uprawnieniami i Uwierzytelniania Użytkowników (CSU), wykazu uprawnień odnotowanych w SysUp oraz raportu z systemu Qasystent. Zbadano uprawnienia do systemu CRCM, SPBD oraz PoltaxPlus. Uprawnienia do systemu CRCM oraz PoltaxPlus nadawane są z wykorzystaniem CSU, w oparciu o koncepcję tzw. ról stanowiskowych (RS). Uprawnienia do systemu SPBD nadawane z wykorzystaniem systemu SysUp.
Badaniu poddano zasadność nadanych ról/uprawnień do ww. systemów pani D. A. i pani W. K.. Szczegółowa analiza wykazała:

- CRCM

Z pracowników wybranych do kontroli uprawnienia do systemu posiadała tylko pani D. A.. Pracownik posiadała rolę przeglądanie oraz analityk.
Naczelnik wyjaśnił, że pracownik weryfikował poprawności złożonych oświadczeń o stanie majątkowym m.in. poprzez porównanie danych z oświadczeń majątkowych z informacjami o posiadanych nieruchomościach pozyskanych z systemu CRCM.

- PoltaxPlus

Pani D. A. w systemie posiadała nadane role stanowiskowe: MIKRO-Oświadczenia majątkowe oraz Pracownik komórki czynności analitycznych i sprawdzających SKA.
Pani W. K. posiadała role stanowiskowe: MIKRO- mandaty, Pracownik komórki czynności analitycznych i sprawdzających SKA oraz Pracownik komórki wymiany informacji międzynarodowej SKM.

- SPBD

Poddani badaniu pracownicy posiadali role w aplikacji: analiza dokumentów oraz analiza podatnika.

Naczelnik wyjaśnił, że zakres posiadanych uprawnień do PoltaxPlus i SPBD wynika z zakresu zadań wykonywanych na stanowiskach pracy ww. pracowników. Niemniej jednak kontrolerzy ustalili, że w badanym okresie pani D. A. nie dokonywała sprawdzeń danych podatników w Poltax oraz SPBD[1].

Nadzór nad ochroną danych osobowych w systemach informatycznych

Z wyjaśnień NUS wynika, że nadzór służbowy nad ochroną danych osobowych w systemach informatycznych dokonywany jest: co kwartał w ramach kontroli zarządczej, co najmniej raz w roku w ramach kontroli funkcjonalnych, przy zmianie zakresów obowiązku wykonywanych zadań.
Na potwierdzenie sprawowania nadzoru w komórce SKA-1, Naczelnik przedstawił dwie karty Informacji o przeprowadzonej kontroli funkcjonalnej, jedna z kontroli przeprowadzonej przez Zastępcę Naczelnika (w dniach 4.08.2023 roku i 28.09.2023 roku) w zakresie: weryfikacja wyrywkowa prawidłowości wykorzystania danych osobowych w systemie SPBD, obejmowała pracowników SKV, SKA-1, SKA-2; druga – z kontroli przeprowadzonej przez kierownika SKA-1 (w zakresie: analiza wpisów CBDiW, obejmowała jedną sprawę prowadzoną przez pracownika D. A.. W pierwszej kontroli nie stwierdzono nieprawidłowości, w drugiej – błędnie wpisano znak sprawy, jest „228- SKA-1….", powinno być „2208-SKA-1…". Błąd wynikał z omyłki pisarskiej.
Naczelnik przedstawił również Tabelę monitorowania kontroli zarządczej obejmującą kontrolowany okres (za III kwartał 2023 roku), w której oświadczył, że pracownicy posiadali aktualne uprawnienia do systemów informatycznych, a także przykładowe wydruki z systemów wniosków o nadanie/odebranie/zmianę uprawnień przy zmianie zakresów obowiązków pracowników.
Z przedłożonych przez NUS dowodów wynika również, że w jednostce prowadzone były działania profilaktyczne – na naradach omawiano zagadnienia dotyczące bezpieczeństwa i ochrony informacji, w tym incydenty bezpieczeństwa, które wystąpiły w IAS, zasady minimalizacji danych oraz pozostałych zasad ochrony danych osobowych. W dniu 10.11.2023

Pisma: (…) z 10.11.2023 roku , (…) z 10.11.2023 roku oraz (…) z 22.11.2023 roku

roku Zastępca Naczelnika wraz z ABI przeprowadzili kontrolę funkcjonalną we wszystkich pomieszczeniach urzędu w zakresie przestrzegania ochrony danych osobowych. W związku z niewłaściwym zabezpieczeniem dokumentów i pieczątek (w dwóch pokojach) wydano zalecenia pokontrolne, wskazano termin realizacji.

Wykorzystanie systemów informatycznych do celów służbowych

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

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

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

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

Badanie oparto na informacjach przekazanych pismami z 22 listopada 2023 roku przez Ministerstwo Finansów Departament Poboru Podatków[2] oraz z 29 listopada 2023 roku przez Ministerstwo Finansów Departament Zwalczania Przestępczości Ekonomicznej.[3]

[2] Pismo (...) z 22.11.2023 roku z załącznikami,

[3] Pismo (...) z 29 listopada 2023 roku z załącznikami,

Na cele kontroli udostępniono dane z następujących systemów informatycznych: SPBD, Poltax oraz CRCM – w zakresie danych podmiotów przeglądanych przez wytypowanych pracowników. Zbadano podstawę do wykorzystania w celach służbowych przedmiotowych danych. Poniżej znajdują się ustalenia dotyczące poszczególnych systemów informatycznych.

1. **SPBD**

W badanym okresie tylko jeden pracownik, W. K., dokonała sprawdzeń w SPBD, w module analiza dokumentów, dotyczyło ono 8 podmiotów. W przypadku 7 podmiotów kontrolowany udokumentował związek przeglądania danych z realizowanymi czynnościami służbowymi. W 1 przypadku pracownik oświadczył, że dokonał sprawdzenia w celu ustnego potwierdzenia podatnikowi (swojemu koledze), że jego zeznanie/zeznania zostały złożone w urzędzie.
Kontrolerzy ustalili, że logując się do aplikacji, w każdym przypadku pracownik wskazał jeden numer sprawy: (…).

Według wyjaśnień NUS, w momencie dokonywania w VIES oceny ryzyka nie ma założonej sprawy w SZD, dlatego dla celów identyfikacji, pracownicy dokonujący oceny wpisywali jeden, ww. numer.

(dowód: pismo NUS – SZD, UNP:2201-23-174181)

<u>Uwagi kontrolerów</u>
Nie uznano wyjaśnień. Aplikacja SPBD służy wykonywaniu zapytań do baz danych Poltax rozproszonych w wielu lokalizacjach. Wdrożenie tego rozwiązania miało na celu uproszczenie procedury dostępu oraz znaczne skrócenie czasu potrzebnego na pozyskanie przekrojowej informacji dotyczącej badanej sprawy lub podmiotu, czyli do pozyskania informacji niezbędnych do wykonania zleconego zadania. Moduł analiza dokumentów w aplikacji SPBD daje dostęp do dokumentów podatnika, możliwość wyświetlenia lub wydrukowania dowolnej deklaracji złożonej w dowolnym urzędzie wraz z danymi szczegółowymi. Dane pozyskane z aplikacji nie mogą być źródłem informacji dla innych celów.
Kontrolerzy ustalili, że w jednym przypadku przeglądanie danych nie miało związku z realizowanymi czynnościami służbowymi, pracownik sprawdzał dokumenty podatnika złożone w innym urzędzie. Niewiarygodne są wyjaśnienia pracownika, że sprawdzał tylko, czy do urzędu wpłynęły zeznania roczne jego kolegi. W trakcie kontroli stwierdzono, że pracownik przeglądał dane szczegółowe zeznań rocznych złożonych w Urzędzie Skarbowym w Wejherowie za lata 2014-2015, 2018-2022.
Przeglądanie danych niezwiązanych z realizowanymi czynnościami służbowymi stanowi nieprawidłowość i narusza zasadę poufności oraz ochrony danych osobowych. Nieuprawniony dostęp do danych podmiotu w SPBD stanowi potencjalny incydent bezpieczeństwa informacji. Zgodnie z zasadami odpowiedzialności, określonymi w Polityce Ochrony Danych Osobowych IAS w Gdańsku, osobami odpowiedzialnymi za przetwarzanie danych osobowych z naruszeniem prawa są wszyscy użytkownicy.

Nie uznano również wyjaśnień NUS dotyczących wpisywania jednego numeru sprawy .W celu uzyskania dostępu do dokumentów podatnika, aplikacja wymaga wprowadzenia numeru

identyfikacyjnego i podania numeru prowadzonej sprawy. Właściwe określenie sprawy jest warunkiem spełnienia zasady rozliczalności. Tymczasem kontrolujący ustalili, że pod nr (…) zarejestrowane są w SZD dwie sprawy, obie mają inny temat, obie zakończone przed kontrolowanym okresem (9.01.2023 roku oraz 17.01.2023 roku). Oznaczenie sprawy niezgodnie ze stanem faktycznym jest nieprawidłowością i narusza zasadę rozliczalności.
Zgodnie z zasadami odpowiedzialności, określonymi w Polityce Ochrony Danych Osobowych IAS w Gdańsku, osobami odpowiedzialnymi za naruszenie powyższej zasady są wszyscy użytkownicy/pracownicy oraz bezpośredni przełożony.

2. Poltax

W badanym okresie tylko jeden pracownik, W. K., dokonała sprawdzeń w podsystemie Poltax, zakres informacji: wyświetlanie informacji o osobie fizycznej, dotyczyło ono 5 podmiotów. We wszystkich przypadkach przeglądanie danych miało związek z wykonywaniem czynności służbowych, z zachowaniem zasad bezpieczeństwa informacji.

3. CRCM

W badanym okresie tylko jeden pracownik, D. A., dokonała sprawdzeń w systemie CRCM. Kontrolerzy ustalili, że pracownik sprawdzał czynności majątkowe 152 podmiotów, w tym 1 podmiotu trzykrotnie, 10 podmiotów dwukrotnie. Pracownik wykonał łącznie 163 logowania do CRCM. W trakcie kontroli zbadano zasadność wszystkich logowań.

W 149 przypadkach przeglądanie danych miało związek z wykonywaniem czynności służbowych, z zachowaniem zasad bezpieczeństwa informacji, przy czym:

- ✓ w jednym przypadku sprawdzenie nie było związane z żadną sprawą. Według wyjaśnień pracownika dane zostały wyszukane omyłkowo w związku z analizą oświadczenia majątkowego innej osoby o podobnym nazwisku – wyjaśnienia uznano,
- ✓ w jednym przypadku sprawdzenie było związane z analizą oświadczenia majątkowego innej osoby. Z wyjaśnień pracownika wynika, że w analizowanym oświadczeniu nie wykazano zadeklarowanego w poprzednich latach samochodu, dlatego pracownik sprawdził we Wro-System w bazie UFG, kto jest nowym właścicielem, a następnie sprawdził, czy w CRCM widnieje informacja o nabyciu tego samochodu. Na potwierdzenie wyjaśnień NUS przedstawił stosowne dokumenty. Wyjaśnienia uznano.

Kontrolerzy ustalili, że w dwóch przypadkach przeglądanie danych nie było związane z żadną konkretną sprawą. Z wyjaśnień pracownika wynika, że sprawdzenia były związane z przydzielonymi pracownikowi sprawami dotyczącymi zakupu pojazdów o wartości powyżej 100 tyś. zł (informacje sygnalne). Kontrolowana jednostka jednak nie jest w stanie udokumentować powiązania tych czynności z żadną sprawą. Brak możliwości udokumentowania związku przeglądanych danych z realizowanymi zadaniami służbowymi jest nieprawidłowością i narusza zasadę rozliczalności.

Zgodnie z zasadami odpowiedzialności, określonymi w Polityce Ochrony Danych Osobowych IAS w Gdańsku, osobami odpowiedzialnymi za naruszenie zasady rozliczalności są użytkownik oraz bezpośredni przełożony w zakresie nadzoru nad czynnościami użytkownika w systemie.

W toku kontroli ustalono ponadto, że w 12 przypadkach pracownik przeglądał czynności majątkowe podmiotów, wobec których nie wykonywał zadań służbowych. W złożonych wyjaśnieniach pracownik potwierdził, że przeglądanie realizowało cel prywatny, a nie służbowy:

- ✓ w 1 przypadku sprawę prowadził inny pracownik, natomiast pani D. A. z powodu zainteresowania sprawą przejrzała podatnika w CRCM,
- ✓ w pozostałych 11 przypadkach (dot. 8 podmiotów, w tym 1 podmiot przeglądany trzykrotnie, 1 dwukrotnie), przeglądane podmioty to znajomi pani D. A. lub jej daleka rodzina, czynności majątkowe odczytała z ciekawości.

[dowód: wyjaśnienia z 11.12.2023 roku w SZD, UNP: 2201-23-179053]

Powyższe jest nieprawidłowością i stanowi incydent bezpieczeństwa – naruszenie zasady poufności oraz naruszenie ochrony danych osobowych.
Zgodnie z zasadami odpowiedzialności, określonymi w Polityce Ochrony Danych Osobowych IAS w Gdańsku, osobami odpowiedzialnymi za naruszenie zasady poufności przetwarzanych danych osobowych są wszyscy użytkownicy/pracownicy oraz bezpośredni przełożony.

Ustalenia:

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

1. naruszenie zasady poufności oraz ochrony danych osobowych w 13 przypadkach – 1 przypadek niezgodnego z prawem przeglądania danych w SPBD w module analiza dokumentów i 12 przypadków przeglądania danych w CRCM,
2. naruszenie zasady rozliczalności – we wszystkich kontrolowanych przypadkach stwierdzono oznaczenia sprawy w SPBD niezgodnie ze stanem faktycznym,
3. nie zrealizowanie polecenia Dyrektora IAS w Gdańsku dotyczącego realizacji w wyznaczonym terminie szkoleń przez panią D. A. w zakresie RODO Unijne rozporządzenie o ochronie danych osobowych oraz bezpieczeństwo teleinformatyczne.

Ustalenia kontroli wykazały, że nadzór sprawowany przez bezpośredniego przełożonego nad czynnościami przetwarzania danych uzyskanych za pośrednictwem systemów informatycznych przez pracowników wytypowanych do kontroli jest niewystarczający.

Osoby odpowiedzialne za stwierdzone nieprawidłowości:

- ✓ pani W. K., pani D. A. w zakresie niezgodnego z prawem przeglądania danych w systemach informatycznych,
- ✓ pani W. K. w zakresie niezgodnego ze stanem faktycznym oznaczania spraw w SPBD,
- ✓ pani O. N., kierownik SKA-1, w zakresie niedostatecznego nadzoru nad czynnościami użytkowników w systemach informatycznych.

Stan prawny:

- ✓ Regulamin Organizacyjny Pierwszego Urzędu Skarbowego w Gdyni stanowiący załącznik do Zarządzenia nr (…) Dyrektora Izby Administracji Skarbowej w Gdańsku z dnia 31 marca 2023 roku w sprawie nadania Regulaminu Organizacyjnego Pierwszemu Urzędowi Skarbowemu w Gdyni (obowiązujący od 1.04.2023 roku do 30.06.2023 roku);
- ✓ Regulamin Organizacyjny Pierwszego Urzędu Skarbowego w Gdyni stanowiący załącznik do Zarządzenia nr (…) Dyrektora Izby Administracji Skarbowej w Gdańsku z dnia 27 czerwca 2023 roku w sprawie nadania Regulaminu Organizacyjnego Pierwszemu Urzędowi Skarbowemu w Gdyni (obowiązujący od 1.07.2023 roku do nadal);
- ✓ Zarządzenie Ministra Finansów, Funduszy i Polityki Regionalnej z dnia 29 grudnia 2020 roku w sprawie wprowadzenia Polityki Ochrony Danych Osobowych;
- ✓ Polityka Ochrony Danych Osobowych Izby Administracji Skarbowej w Gdańsku stanowiąca załącznik do zarządzenia nr (…) Dyrektora Izby Administracji Skarbowej w Gdańsku z dnia 16 czerwca 2020 roku (obowiązująca od 16.06.2020 roku do 17.09.2023 roku);
- ✓ Polityka Ochrony Danych Osobowych Izby Administracji Skarbowej w Gdańsku stanowiąca załącznik do zarządzenia nr (…) Dyrektora Izby Administracji Skarbowej w Gdańsku z dnia 18 września 2023 roku (obowiązująca od 18.09.2023 roku do nadal);
- ✓ Zarządzenie Ministra Finansów z dnia 10 marca 2022 roku w sprawie Systemu Zarządzania Bezpieczeństwem Informacji i Polityki Bezpieczeństwa Informacji Resortu Finansów;
- ✓ Zarządzenie Ministra Finansów z dnia 25 lipca 2022 roku zmieniającej zarządzenie w sprawie Systemu Zarządzania Bezpieczeństwem Informacji i Polityki Bezpieczeństwa Informacji Resortu Finansów;
- ✓ Polityka Bezpieczeństwa Informacji w Izbie Administracji Skarbowej w Gdańsku, wprowadzona zarządzeniem nr (…) DIAS w Gdańsku z dnia 25 maja 2018 roku;
- ✓ Polityka Bezpieczeństwa Teleinformatycznego Resortu Finansów z 27.12.2022 roku;
- ✓ Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 (RODO) z dnia 27 kwietnia 2016 roku 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);
- ✓ Decyzja nr (…) Dyrektora Izby Administracji Skarbowej w Gdańsku z dnia 22 grudnia 2021 roku w sprawie powołania Zespołu ds. Systemu Zarządzania Bezpieczeństwem Informacji w Izbie Administracji Skarbowej w Gdańsku;
- ✓ Decyzja nr (…) Dyrektora Izby Administracji Skarbowej w Gdańsku z dnia 2 marca 2023 roku w sprawie wyznaczenia merytorycznych aplikacji/systemów informatycznych oraz koordynatorów merytorycznych i ich zastępców.

III. Zalecenia

Przedstawiając powyższe ustalenia kontroli Dyrektor Izby Administracji Skarbowej w Gdańsku poleca:

1) Wdrożyć rozwiązania organizacyjne zapewniające pełną rozliczalność przetwarzanych (przeglądanych) danych w systemach informatycznych. Należy objąć nadzorem prawidłowość wykonywanych zapytań w systemie.
2) Zwiększyć nadzór nad realizacją szkoleń w wyznaczonych terminach przez pracowników oraz objąć ten obszar kontrolą funkcjonalną.
3) Zintensyfikować kontrole funkcjonalne w zakresie zagadnień związanych z ochroną danych osobowych,
4) Rozważyć zasadność posiadania uprawnień w SPBD przez panią D. A..

Na podstawie art. 49 ustawy o kontroli w administracji rządowej, w nawiązaniu do przedstawionych powyżej ustaleń kontroli, proszę o przedłożenie w terminie 1 miesiąca od daty otrzymania niniejszego sprawozdania z kontroli informacji o sposobie wykorzystania zaleceń, wykorzystania wniosków lub przyczynach ich niewykorzystania albo o innym sposobie usunięcia stwierdzonych nieprawidłowości. Informacje w powyższym zakresie powinny wskazywać konkretne działania i sposób ich realizacji.

Jednocześnie w związku z poleceniem Ministerstwa Finansów zobowiązuję do przekazania do kierownika komórki ds. kontroli tut. Izby Administracji Skarbowej informacji o rezultatach wdrożonych zaleceń pokontrolnych w terminie 9 miesięcy licząc od daty sporządzenia przez jednostkę kontrolowaną informacji o zrealizowaniu zaleceń pokontrolnych.

IV. Pozostałe informacje

Zgodnie z art. 52 ust. 5 ustawy o kontroli w administracji rządowej Kierownik jednostki kontrolowanej w terminie 3 dni roboczych od dnia otrzymania sprawozdania ma prawo przedstawić do niego stanowisko; nie wstrzymuje to realizacji ustaleń kontroli.

Sprawozdanie z kontroli zostało sporządzone w formie elektronicznej, przesłane do kierownika jednostki kontrolowanej za pośrednictwem Systemu Zarządzania Dokumentami (SZD).

Gdańsk, dnia 9 stycznia 2024 roku

Z wyrazami szacunku
Dyrektor Izby Administracji Skarbowej w Gdańsku

Barbara Bętkowska-Cela
(podpisano kwalifikowanym podpisem elektronicznym)