Załącznik nr 21
do instrukcji I-086/3

Krajowa Administracja Skarbowa

Izba Administracji Skarbowej w Gdańsku

2201-IWW[1].0921.21.2023

UNP: 2201-23-147776

WYSTĄPIENIE POKONTROLNE

Izba Administracji Skarbowej w Gdańsku

F-391/3 - Wystąpienie pokontrolne kontroli prowadzonej w urzędach skarbowych woj. pomorskiego oraz w Pomorskim Urzędzie Celno-Skarbowym w Gdyni

Temat kontroli: „Ocena zasadności przetwarzania danych przez pracowników i funkcjonariuszy za pośrednictwem systemów informatycznych”

Jednostka kontrolowana:
Urząd Skarbowy w Chojnicach
Ul. Młyńska 22
89-600 Chojnice

Kierownik jednostki kontrolowanej:

1. Pan Aleksander Ciepliński
   Naczelnik Urzędu Skarbowego w Chojnicach (zwany dalej Naczelnikiem lub NUS) powołany na stanowisko Naczelnika od 26.10.2022 r.
2. Pani Honorata Szwak
   Zastępca Naczelnika, pełni tę funkcję od 14.11.2022 r.

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]1.0921.21.2023 z 10.08.2023 r.

Data rozpoczęcia czynności kontrolnych: 11.08.2023 r.
Data zakończenia czynności kontrolnych: 15.09.2023 r.

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

Wpisano do ewidencji kontroli pod poz. 1/2023

Okres objęty kontrolą od 1.01.2023 r. do 30.06.2023 r. Badaniem zostały objęte również zdarzenia i dokumenty wcześniejsze lub późniejsze, gdy miały związek z przedmiotem kontroli.

Zakres przedmiotowy kontroli:
Zakres badania obejmuje następujące zagadnienia kontroli:
1) Organizacja pracy urzędu w zakresie korzystania z systemów informatycznych;
2) Wykorzystanie systemów informatycznych do celów służbowych;
3) Nadzór nad prawidłowością wykorzystania danych z systemów informatycznych w ramach kontroli funkcjonalnej.

I. Ocena kontrolowanej działalności

Ocena ogólna:

Działania kierowanego przez Naczelnika Urzędu Skarbowego w Chojnicach w badanym zakresie oceniono **pozytywnie z nieprawidłowościami.**

Uzasadnienie oceny ogólnej:

Wpływ na ocenę ogólną skontrolowanego zakresu miały stwierdzone nieprawidłowości:

1. Nie zapoznanie się pracowników z Polityką Ochrony Danych Osobowych.
2. Nie odbycie obowiązkowych szkoleń przez wszystkich pracowników w wyznaczonym przez DIAS terminie.
3. Nieuzasadnione nadanie pracownikowi uprawnień dedykowanych kierownikowi.
4. Naruszenie zasad dostępności i poufności.
5. Wykorzystywanie danych z systemu niezgodnie z przeznaczeniem.
6. Nie prowadzenie nadzoru nad prawidłowością wykorzystania danych z systemów informatycznych w ramach kontroli funkcjonalnej.

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

II. Opis ustalonego stanu faktycznego

Zagadnienie <u>pierwsze</u> z zakresu badania Organizacja pracy urzędu w zakresie korzystania z systemów informatycznych.

Opis stanu faktycznego:

W Urzędzie Skarbowym w Chojnicach 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 Urzędu Skarbowego w Chojnicach stanowiący załącznik do Zarządzenia nr 143/2022 Dyrektora Izby Administracji Skarbowej w Gdańsku z dnia 23 grudnia 2022 roku w sprawie nadania Regulaminu Organizacyjnego Urzędowi Skarbowemu w Chojnicach (obowiązujący od 1.01.2023 r. do 28.02.2023 r.);
- ✓ Regulamin Organizacyjny Urzędu Skarbowego w Chojnicach stanowiący załącznik do Zarządzenia nr 22/2023 Dyrektora Izby Administracji Skarbowej w Gdańsku z dnia 2 marca 2023 roku w sprawie nadania Regulaminu Organizacyjnego Urzędowi Skarbowemu w Chojnicach (obowiązujący od 1.03.2023 r. do 30.04.2023 r.);
- ✓ Regulamin Organizacyjny Urzędu Skarbowego w Chojnicach stanowiący załącznik do Zarządzenia nr 36/2023 Dyrektora Izby Administracji Skarbowej w Gdańsku z dnia 24 kwietnia 2023 roku w sprawie nadania Regulaminu Organizacyjnego Urzędowi Skarbowemu w Chojnicach (obowiązujący od 1.05.2023 r. do nadal).

Zgodnie ze strukturą organizacyjną urzędu Naczelnik Urzędu sprawuje bezpośredni nadzór nad:

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

Zastępca Naczelnika sprawuje bezpośredni nadzór nad:

1. Pionem Kontroli i Orzecznictwa (SZNKP):
   - ✓ Działem Czynności Analitycznych i Sprawdzających oraz Identyfikacji i Rejestracji Podatkowej (SKA-1),
   - ✓ Referatem Czynności Analitycznych i Sprawdzających (SKA-2),
   - ✓ Działem Postępowania Podatkowego i Kontroli Podatkowej (SPO).

W kontrolowanym zakresie szczegółowym badaniem objęto kierowników i pracowników:

- ✓ Referatu Identyfikacji i Rejestracji Podatkowej (SKI) - komórka funkcjonowała w okresie 01.01.2023 r. – 28.02.2023 r., którą kierowała Pani J. G.. Podczas nieobecności zastępowała ją Pani P. P.. Zadania komórki realizowało 5 pracowników (łącznie z kierownikiem komórki),
- ✓ Pierwszego Referatu Czynności Analitycznych i Sprawdzających (SKA-1) - komórka funkcjonowała w okresie 01.01.2023 – 28.02.2023 r., którą kierował Pan K. W.. Podczas nieobecności zastępowały go Pani E. L. (pierwszy zastępca) oraz Pani K. C. (drugi zastępca kierownika w sytuacji nieobecności kierownika oraz jego pierwszego zastępcy). Zadania referatu realizowało 8 pracowników (łącznie z kierownikiem),
- ✓ Działu Czynności Analitycznych i Sprawdzających oraz Identyfikacji i Rejestracji Podatkowej (SKA-1) – komórka powstała od 01.03.2023 r. z połączenia komórek SKI oraz SKA-1, którą kierował pełniący obowiązki kierownika Pan K. W., Podczas nieobecności zastępowały go Pani E. L. (pierwszy zastępca) oraz Pani K. C. (drugi zastępca kierownika w sytuacji nieobecności kierownika oraz jego pierwszego zastępcy). Zadania komórki realizowało 11 pracowników (łącznie z kierownikiem).

Według Regulaminu organizacyjnego Urzędu Skarbowego w Chojnicach, 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 r.,
- ✓ Polityka Bezpieczeństwa Informacji w Izbie Administracji Skarbowej w Gdańsku, wprowadzona zarządzeniem nr (…) DIAS w Gdańsku z dnia 25 maja 2018 r.,
- ✓ Decyzja nr (…) Dyrektora Izby Administracji Skarbowej w Gdańsku z dnia 5 lipca 2022 r. 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 r. 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 r. w sprawie wyznaczenia merytorycznych aplikacji/systemów informatycznych oraz koordynatorów merytorycznych i ich zastępców,

- ✓ Decyzja nr (…) Dyrektora Izby Administracji Skarbowej w Gdańsku z dnia 31 października 2022 r. w sprawie wyznaczenia koordynatora lokalnego Krajowego Systemu Informatycznego w Izbie Administracji Skarbowej w Gdańsku.

Koordynator do spraw ochrony danych osobowych

Na podstawie Decyzji nr (…) Dyrektora Izby Administracji Skarbowej w Gdańsku z dnia 5 lipca 2022 r. w sprawie wyznaczenia pracowników do spraw bezpieczeństwa danych osobowych w Izbie Administracji Skarbowej w Gdańsku, w urzędach skarbowych woj. pomorskiego oraz Pomorskim Urzędzie Celno – Skarbowym, w Urzędzie Skarbowym w Chojnicach, osobą odpowiedzialną za realizację zadań z zakresu ochrony danych osobowych jest Pan K. W., kierownik działu czynności analitycznych i sprawdzających oraz identyfikacji i rejestracji podatkowej. Nie wyznaczono osoby zastępującej.

[Dowód: decyzja nr (…) DIAS, Qasystent)]

Zapoznanie pracowników 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 r. (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 r. zobowiązał wszystkich pracowników do zapoznania z treścią Polityki za pośrednictwem systemu Qasystent w terminie do 12 lutego 2021r. i potwierdzenia tego faktu w powyższym systemie.

W systemie Qasystent zapoznało się i potwierdziło ten fakt 64 pracowników (na 70 pracowników zobowiązanych do zapoznania).
6 pracowników nie zapoznało się z zarządzeniem, tj.:

1. M. A. - w okresach od 21.02.2020 r. do 24.09.2021 r oraz od 31.12.2021 r. do nadal długotrwale nieobecna. Pracownik był obecny w pracy w okresie od 27.09.2021 r. do 30.12.2021 i miał obowiązek oraz możliwość zapoznania się z zarządzeniem,
2. A. L. – pracownik od 23.02.2023 r. do nadal jest długotrwale nieobecny. Na dzień wyznaczonego terminu zapoznania się z zarządzeniem był obecny i nie wypełnił obowiązku zapoznania się z dokumentem,
3. D. M. - pracownik od 18.05.2022 r. do nadal jest długotrwale nieobecny. Na dzień wyznaczonego terminu zapoznania się z zarządzeniem był obecny i nie wypełnił obowiązku zapoznania się z dokumentem,
4. K. S. - pracownik od 01.04.2021 r. do nadal jest długotrwale nieobecny. Na dzień wyznaczonego terminu zapoznania się z zarządzeniem był obecny i nie wypełnił obowiązku zapoznania się z dokumentem,
5. E. S. - pracownik od 15.11.2021 r. do nadal jest długotrwale nieobecny. Na dzień wyznaczonego terminu zapoznania się z zarządzeniem był obecny i nie wypełnił obowiązku zapoznania się z dokumentem,

6. M. Z. - pracownik od 27.09.2021 r. do nadal jest długotrwale nieobecny. Na dzień wyznaczonego terminu zapoznania się z zarządzeniem był obecny i nie wypełnił obowiązku zapoznania się z dokumentem.

Brak zapoznania się z Polityką stanowi nieprawidłowość, polegającą na nie zrealizowaniu polecenia Dyrektora.

Naczelnik wyjaśnił, że przyczyną braku zapoznania pracowników z zarządzeniami są m.in. zmiany kadrowe pracowników, w szczególności kadry kierowniczej, przesunięcia pracowników do innych zadań i innych komórek, a także duża ilość obowiązków, szczególnie w akcji PIT, kiedy to przypadał termin zapoznania się Polityką Ochrony Danych Osobowych. Naczelnik wskazał, że główną przyczyna braku zapoznania się pracowników z Polityka Ochrony Danych Osobowych stanowi fakt umieszczenia dokumentu w zakładce „ dokumentacja zewnętrzna" w aplikacji Qasystent. Z tej zakładki dokumenty nie ukazywały się na startowej stronie aplikacji, w przeciwnym razie każdy z pracowników zapoznałby się z treścią dokumentu.
Ponadto, Naczelnik poinformował, że od lipca 2023 polecił kierownikom sporządzanie comiesięcznych raportów z aplikacji Qasystent o zapoznaniu się z pracowników z dokumentacją.

(dowód: pismo NUS – SZD, UNP:2201-23-124927)

Uwagi kontrolerów
Wyjaśnienia Naczelnika nie zmieniają ustaleń kontroli. Dyrektor pismem nr (…) z 26.01.2021 r. zobowiązał wszystkich pracowników do zapoznania z treścią Polityki, w którym wyznaczył ponad dwutygodniowy termin do zapoznania się oraz wskazał w jakiej aplikacji należy to zrealizować.
Biorąc pod uwagę ustalenia kontroli oraz złożone wyjaśnienia przez Naczelnika, stwierdza się, że nadzór nad realizacją polecenia Dyrektora był niewystarczający, co skutkowało nie zapoznaniem się w wyznaczonym terminie z Polityką przez wszystkich pracowników.
Pozytywnie należy ocenić działania podjęte od lipca 2023 roku przez Naczelnika w kierunku zwiększenia nadzoru nad obowiązkiem zapoznawania się z wymaganą dokumentacją przez podległych pracowników.

Obowiązkowe szkolenia do pracowników

Dyrektor Izby Administracji Skarbowej w Gdańsku w pismach kierowanych do Naczelnika Urzędu, polecił wszystkim pracownikom do odbycia szkoleń z zakresu:
1) RODO Unijne rozporządzenie o ochronie danych osobowych – dostępne na platformie e-learningowej Atena2, wyznaczony termin: 30.04.2018 r. Zobowiązanych do odbycia szkolenia było 74 pracowników. Szkolenie ukończyło 68 pracowników, w tym 8 pracowników[1] dopiero w trakcie kontroli. Pozostałych 6 pracowników[2] obecnie długotrwale nieobecnych, nie odbyło szkolenia pomimo, że mieli możliwość zrealizowania szkolenia.
2) Bezpieczeństwo teleinformatyczne - dostępne na platformie e-learningowej Atena2, wyznaczony termin: 30.06.2022 r. Zobowiązanych do odbycia szkolenia było 68 pracowników. Szkolenie

[1]K. C., D. D., Ł. K., D. K., T. M., M. M., L. R., W. T,
[2] J. K., D. M., P. S., E. S., S. S., M. Z.

ukończyło 65 pracowników, w tym 3 pracowników[3] dopiero w trakcie kontroli. 3 pracowników[4] obecnie długotrwale nieobecnych, nie odbyło szkolenia pomimo, że miało możliwość zrealizowania szkolenia.

3) Naruszenie ochrony danych osobowych – dostępne na platformie e-learningowej Moodle, wyznaczony termin: bezzwłocznie. Wszyscy zobowiązani w ilości 68, zrealizowali szkolenie.
4) Zasady bezpieczeństwa informacji - dostępne na platformie e-learningowej Moodle, wyznaczony termin: 13.01.2023 r. Wszyscy zobowiązani w ilości 68, zrealizowali szkolenie.

Powyższe dane ustalono na podstawie stanu zatrudnienia w okresie objętym kontrolą.

Z powyższego wynika, że brak realizacji szkoleń dot. RODO Unijne rozporządzenie o ochronie danych osobowych oraz bezpieczeństwo teleinformatyczne stanowi nieprawidłowość, polegającą na nie zrealizowaniu polecenia Dyrektora.

Naczelnik wyjaśnił, że przyczyną braku ukończenia szkoleń przez pracowników, są m.in. zmiany kadrowe pracowników, w szczególności kadry kierowniczej, przesunięcia pracowników do innych zadań i innych komórek, a także duża ilość obowiązków, szczególnie w akcji PIT, kiedy to przypadał termin odbycia szkolenia z RODO oraz bezpieczeństwa teleinformatycznego. Brak ukończenia szkoleń w wyznaczonych terminach spowodowany był też problemami technicznymi z dostępnością ATENA2 polegającymi na braku możliwości zalogowania się do systemu (aktualnie nie można odbyć szkolenia w domu na prywatnym sprzęcie), a także problemami technicznymi ze strony przeglądarek internetowych, które nie zapisują wyników testów. Naczelnik wskazał również, że okres pandemiczny przyczynił się do opóźnienia w realizacji szkolenia (praca zdalna, opieka rodzicielska nad małoletnimi dziećmi, absencja w wyniku zachorowania na COVID).

(dowód: pismo NUS – SZD, UNP:2201-23-124927)

<u>Uwagi kontrolerów</u>

Wyjaśnienia Naczelnika nie zmieniają ustaleń kontroli, Dyrektor IAS w Gdańsku pismami :

1) nr (…) z 25.01.2018 r. zobowiązał wszystkich pracowników do ukończenia szkolenia e-learningowego dot. RODO Unijne rozporządzenie o ochronie danych osobowych" w nieprzekraczalnym terminie do 30 kwietnia 2018 r. oraz zobowiązał kierowników komórek organizacyjnych do poinformowania nowo zatrudnionych osób o obowiązku odbycia przedmiotowego szkolenia. Czas na realizacje szkolenia wynosił ponad 3 miesiące. Wg ustaleń kontroli, niektórzy pracownicy zrealizowali szkolenie po upływie 5 lat.
2) nr (…) z 12.04.2022 r. polecił zobligowanie podległych pracowników oraz nowo zatrudnianych pracowników do odbycia szkolenia e-learningowego dot. Bezpieczeństwa teleinformatycznego w terminie do 30 czerwca 2022 r. Czas na realizacje szkolenia wynosił ponad 2 miesiące. Wg ustaleń kontroli, niektórzy pracownicy zrealizowali szkolenie po upływie roku.
3) nr (…) z 8.03.2023 r. poinformował, że od 10 marca 2023 roku z serwisu e-learningowego Atena2 będzie można korzystać tylko na urządzeniach służbowych.

[3] R. F., E. L., M. O.,
[4] J. K., M. S., P. S.,

Biorąc pod uwagę powyższe, stwierdza się, że nadzór nad realizacją szkoleń był niewystarczający, co skutkowało nie odbyciem w wyznaczonych terminach szkoleń przez wszystkich pracowników.

Upoważnienie do przetwarzania danych osobowych

Badanie przeprowadzono na podstawie upoważnień i nadanych uprawnień 3 nowozatrudnionym pracownikom[5] oraz 3 pracownikom[6] zwolnionym w kontrolowanym okresie.
Wszyscy pracownicy posiadali w kontrolowanym okresie aktualne upoważnienia do przetwarzania danych osobowych i podpisali stosowne oświadczenie dot. ochrony danych osobowych.[7]
Nowozatrudnionym pracownikom po podpisaniu upoważnień nadano uprawnienia do systemów informatycznych. Upoważnienia pracowników zwolnionych w kontrolowanym okresie utraciły moc z dniem ustania stosunku pracy, w następstwie czego odebrano im uprawnienia w systemach informatycznych.
Upoważnienia zarejestrowane są w ewidencji osób upoważnionych do przetwarzania danych osobowych w aplikacji Portal Pracownika. Ewidencja zawiera stosowne elementy uregulowane w pkt (…) Procedury nadawania i odwoływania upoważnień imiennych do przetwarzania danych osobowych[8].

Uprawnienia do systemów informatycznych

Badanie przeprowadzono na podstawie udostępnionych przez Naczelnika raportu 10 – Raport o uprawnieniach i rolach użytkownika z Centralnego Systemu Zarządzania Uprawnieniami i Uwierzytelniania Użytkowników (CSU) oraz wykazu uprawnień pracowników do systemów nadawanych poza CSU, odnotowanych w SysUp. Zbadano uprawnienia do systemu CRCM oraz SeRCe wszystkich pracowników i kierowników komórek: SKI, SKA-1

Uprawnienia do systemu CRCM nadawane są z wykorzystaniem CSU, w oparciu o koncepcję tzw. ról stanowiskowych (RS). Uprawnienia do systemu SeRCe nadawane z wykorzystaniem systemu SysUp, na podstawie wniosku wygenerowanego w SeRCu.
Badaniu poddano zasadność nadanych uprawnień do systemów: CRCM, SeRCe. Szczegółowa analiza wykazała:

1. CRCM

[5] M. G., W. T., K. Ł.,
[6] K. B., M. S., J. K.,
[7] Pracownicy podpisali oświadczenie o treści: „Potwierdzam odbiór niniejszego upoważnienia oraz zobowiązuję się do zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia, do których uzyskam dostęp w związku z niniejszym upoważnieniem i wykonywaniem powierzonych mi obowiązków – na czas ważności upoważnienia, jak również po jego ustaniu. Ponadto zobowiązuje się do przetwarzania danych zgodnie z przepisami RODO oraz dokumentacji wewnętrznej związanej z ochroną danych osobowych.
[8] Załącznik nr 5 do Polityki Ochrony Danych Osobowych Izby Administracji Skarbowej w Gdańsku stanowiącej załącznik do zarządzenia nr (…) DIAS w Gdańsku z dnia 16 czerwca 2020 r.
Pkt (…)

a) SKI (komórka funkcjonowała w okresie 01.01.2023 r. – 28.02.2023 r.) – uprawnienia do systemu posiadało 3 pracowników[9]. Kierownik SKI posiadał najszersze uprawnienia, tj. analityk, przeglądanie oraz kierownik merytoryczny REJ. Pozostali pracownicy posiadali takie samo uprawnienie, tj. przeglądanie.
Naczelnik wyjaśnił, że uprawnienie wyłącznie do przeglądania w systemie CRCM był niezbędny pracownikom w zakresie weryfikacji złożonego zgłoszenia VAT-R.

b) SKA-1 (komórka funkcjonowała w okresie 01.01.2023 r. – 28.02.2023 r.) – uprawnienia do systemu posiadało 8 pracowników[10]. Kierownik SKA-1 posiadał najszersze uprawnienia, tj. analityk, przeglądanie oraz kierownik merytoryczny REJ. Pozostali pracownicy posiadali takie same uprawnienia, tj. analityk, przeglądanie.
Z wyjaśnień Naczelnika, wynika że w zakresie danych z aplikacji CRCM pracownicy wykonujący zadania z obszaru czynności analitycznych i sprawdzających korzystali z systemu przede wszystkim dokonując analizy zasadności zwrotu VAT, celem sprawdzenia sytuacji majątkowej podatnika.

c) SKA-1 (komórka funkcjonuje od 1.03.2023 r., powstała z połączenia komórek SKI oraz SKA-1) – uprawnienia do systemu posiada jedenastu pracowników[11]. Kierownik posiada najszersze uprawnienia, tj. analityk, przeglądanie, kierownik merytoryczny REJ, kierownik merytoryczny PCC, kierownik merytoryczny PPR, kierownik merytoryczny SD. Dziewięciu pracowników[12] posiada te same uprawnienia tj. analityk, przeglądanie, w tym jeden pracownik[13] posiada również uprawnienie pracownik merytoryczny REJ, a jeden pracownik[14] posiada uprawnienie kierownik merytoryczny REJ. Jeden pracownik[15] posiada tylko uprawnienie przeglądanie.

Naczelnik wyjaśnił, że rodzaj i zakres uprawnień poszczególnych pracowników do systemu uwarunkowane jest organizacją pracy w Referacie. Uprawnienia posiadają obecnie osoby odpowiedzialne za prowadzenie czynności analitycznych i sprawdzających oraz pracownicy prowadzący czynności rejestracyjne oraz weryfikacyjne złożonych zgłoszeń VAT-R. Naczelnik wskazał, że wyznaczył P. P. jako osobę wiodącą w komórce w zakresie zadań związanych z identyfikacją i rejestracją podatkową oraz nadał jej uprawnienia kierownika merytorycznego REJ. Kierownik posiada najszersze uprawnienia celem sprawowania kompleksowego nadzoru nad wykonywaniem zadań przez podległych pracowników.

(dowód: pismo NUS – SZD, UNP: 2201-23-133213)

Uwagi kontrolerów

Nadanie pracownikowi uprawnienia kierownik merytoryczny REJ jest niezgodne z podręcznikiem użytkownika systemu CRCM, z którego wynika wprost, że rola kierownika

[9] J. G., P. P., M. L.,
[10] K.W., E. L., K. C., P. T., B. K., K. F., M. D., M. Ł.,
[11] K.W., E. L., K. C., P. T., B. K., K. F., M. D., M. Ł., M. L., K. Ł.,
[12] K. C., M. D., B. K., K. F., E. L., M. Ł., P. T., K. Ł., P. P.,
[13] K.Łl,
[14] P.P.,
[15] M.L,

merytorycznego REJ przeznaczona jest dla pracowników będącymi kierownikami komórki, poza przypadkiem, gdy jeden z pracowników zastępuje kierownika w czasie jego nieobecności. Pracownik któremu nadano uprawnienia, nie jest wyznaczony do zastępowania kierownika komórki, zatem brak podstaw do nadania mu tak szerokich uprawnień.

2. SeRCe

a) SKI (komórka funkcjonowała w okresie 01.01.2023 r. – 28.02.2023 r.) – uprawnienia do przeglądania i rejestrowania do systemu posiadało 5 pracowników[16]. Nadane uprawnienia umożliwiały pracownikom realizowanie szeregu zadań w zakresie identyfikacji i rejestracji podatkowej.

b) SKA-1 (komórka funkcjonowała w okresie 01.01.2023 r. – 28.02.2023 r.) - uprawnienia do systemu posiadało 8 pracowników[17]. Kierownik komórki oraz pracownicy posiadali uprawnienia związane tylko z przeglądaniem obowiązków podatkowych i przeglądaniem podmiotów. Uprawnienia te były wystarczające w realizacji zadań służbowych.

c) SKA-1 (komórka funkcjonuje od 1.03.2023 r., powstała z połączenia komórek SKI oraz SKA-1) – uprawnienia do systemu posiada jedenastu pracowników[18]. Kierownik oraz pięciu pracowników[19] posiadają najszersze uprawnienia do przeglądania i rejestrowania w systemie, umożliwiające realizację zadań służbowych z zakresu identyfikacji i rejestracji podatkowej. Pozostałych pięciu pracowników [20] realizujących zadania z zakresu czynności sprawdzających i analitycznych posiadają uprawnienia tylko do przeglądania obowiązków podatkowych i danych rejestracyjnych podmiotów, które są wystarczające w realizacji zadań.

Upoważnienia w komórce SKI, SKA-1

W toku kontroli dokonano sprawdzenia upoważnień do działania w imieniu Naczelnika Urzędu Skarbowego w Chojnicach nadanych łącznie 5 pracownikom[21] z komórek SKI, SKA-1 w zakresie prawidłowości podstawy prawnej, odnotowania otrzymania do wiadomości upoważnienia przez pracowników i aktualności upoważnienia. Badaniem objęto upoważnienia obowiązujące w kontrolowanym okresie.
Badane upoważniania zawierały prawidłowe podstawy prawne oraz zostały podpisane przez osoby do tego upoważnione. Na wszystkich badanych upoważnieniach pracownicy potwierdzili odbiór własnoręcznym podpisem (z datą). Upoważnienia obowiązują od dnia podpisania do odwołania lub do dnia rozwiązania umowy o pracę.

Ustalenia:

[16] J. G., P. P., M. L., K. B., P. S,
[17] K.W., E. L., K. C., P. T., B. K., K. F., M. D., M. Ł,
[18] K.W. E. L., K. C., P. T., B. K., K. F., M. D., M. Ł., P. P., M. L., K. Ł.,,
[19] K.W. E. L., B. K., K. F., P. P., M. L.,,
[20] K. C., P. T., M. D., M. Ł., K. Ł.,,
[21] J. G. (kierownik SKI do 28.02.2023 r.), P. P. (zastępca kierownika SKI do 28.02.2023 r.), K. W. (p.o. kierownik SKA-1 od 01 marca 2023 r.), E. L. (pierwszy zastępca p.o. kierownika SKA-1 od 1 marca 2023 r.), K. C. (drugi zastępca p.o. kierownika SKA-1 od 1 marca 2023 r.),

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

1. Nie zapoznanie się z Polityką Ochrony Danych Osobowych przez 6 pracowników[22] ,
2. 6 pracowników[23] nie odbyło szkolenia na platformie e-learningowej Atena2 pt. RODO Unijne rozporządzenie o ochronie danych osobowych w wyznaczonym przez DIAS terminie, 8 pracowników[24] odbyło szkolenie dopiero w trakcie kontroli,
3. 3 pracowników[25] nie odbyło szkolenia na platformie e-learningowej Atena2 pt. Bezpieczeństwo teleinformatyczne w wyznaczonym przez DIAS terminie, 3 pracowników[26] odbyło szkolenie dopiero w trakcie kontroli,
4. Nadanie pracownikowi[27] w systemie CRCM uprawnienia kierownika merytorycznego REJ, przeznaczonego dla kierownika komórki.

Ocena cząstkowa:

Działalność Urzędu Skarbowego w Chojnicach należy ocenić ***pozytywnie z nieprawidłowościami***

Stan prawny:

- ✓ Regulamin Organizacyjny Urzędu Skarbowego w Chojnicach stanowiący załącznik do Zarządzenia nr 143/2022 Dyrektora Izby Administracji Skarbowej w Gdańsku z dnia 23 grudnia 2022 roku w sprawie nadania Regulaminu Organizacyjnego Urzędowi Skarbowemu w Chojnicach (obowiązujący od 1.01.2023 r. do 28.02.2023 r.);
- ✓ Regulamin Organizacyjny Urzędu Skarbowego w Chojnicach stanowiący załącznik do Zarządzenia nr 22/2023 Dyrektora Izby Administracji Skarbowej w Gdańsku z dnia 2 marca 2023 roku w sprawie nadania Regulaminu Organizacyjnego Urzędowi Skarbowemu w Chojnicach (obowiązujący od 1.03.2023 r. do 30.04.2023 r.);
- ✓ Regulamin Organizacyjny Urzędu Skarbowego w Chojnicach stanowiący załącznik do Zarządzenia nr 36/2023 Dyrektora Izby Administracji Skarbowej w Gdańsku z dnia 24 kwietnia 2023 roku w sprawie nadania Regulaminu Organizacyjnego Urzędowi Skarbowemu w Chojnicach (obowiązujący od 1.05.2023 r. do nadal) ;
- ✓ Zarządzenie Ministra Finansów, Funduszy i Polityki Regionalnej z dnia 29 grudnia 2020 r. w sprawie wprowadzenia Polityki Ochrony Danych Osobowych;
- ✓ Polityka Ochrony Danych Osobowych Izby Administracji Skarbowej w Gdańsku stanowiącej załącznik do zarządzenia nr (…) Dyrektora Izby Administracji Skarbowej w Gdańsku z dnia 16 czerwca 2020 r.;
- ✓ Zarządzenie Ministra Finansów z dnia 10 marca 2022 r. w sprawie Systemu Zarządzania Bezpieczeństwem Informacji i Polityki Bezpieczeństwa Informacji Resortu Finansów;
- ✓ Zarządzenie Ministra Finansów z dnia 25 lipca 2022 r. zmieniającej zarządzenie w sprawie Systemu Zarządzania Bezpieczeństwem Informacji i Polityki Bezpieczeństwa Informacji Resortu Finansów;

[22] M. A., A. L., D. M., K. S., E. S., M. Z,
[23] [23] J. K., D. M., P. S., E. S., S. S., M. Z.

[24] K. C., D. D., Ł. K., D. K., T. M., M. M., L. R., W. T.,
[25] J. K., M. S., P. S.,,
[26] R. F., E. L., M. O.,,
[27] P.P.

- ✓ Polityka Bezpieczeństwa Informacji w Izbie Administracji Skarbowej w Gdańsku, wprowadzona Zarządzeniem nr (…) DIAS w Gdańsku z dnia 25 maja 2018 r.;
- ✓ Polityka Bezpieczeństwa Teleinformatycznego Resortu Finansów z 27.12.2022 r.;
- ✓ Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 (RODO) 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);
- ✓ Decyzja nr (…) Dyrektora Izby Administracji Skarbowej w Gdańsku z dnia 5 lipca 2022 r. 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.

Zagadnienie <u>drugie</u> z zakresu badania: *Wykorzystanie systemów informatycznych do celów służbowych.*

Opis stanu faktycznego:

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

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

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

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

Badanie oparto na informacjach przekazanych pismami z 18 sierpnia 2023 r. przez Departament Poboru Podatków Ministerstwa Finansów[28] oraz z 22 sierpnia 2023 r. przez Departament Zwalczania Przestępczości Ekonomicznej Ministerstwa Finansów.[29]
Na cele kontroli udostępniono dane z następujących systemów informatycznych: SeRCe, CRCM – w zakresie danych podmiotów przeglądanych przez wytypowanych pracowników komórek SKI oraz SKA-1. Zbadano podstawę do wykorzystania w celach służbowych przedmiotowych danych. Poniżej znajdują się ustalenia dotyczące poszczególnych systemów informatycznych.

1. SeRCe

Badanie przeprowadzono na próbie 15 podmiotów przeglądanych przez trzech pracowników[30]. Na podstawie złożonych wyjaśnień potwierdzonych stosownymi dokumentami ustalono, że we wszystkich przypadkach sprawdzenie miało związek z ustalaniem właściwości miejscowej organu podatkowego, aktualizacją danych, weryfikacją adresu w związku z rozbieżnością pomiędzy danymi wykazanymi w deklaracjach a SeRCem, sprawdzeniem numeru kontaktowego w związku z czynnościami sprawdzającymi dot. VAT-7.

Na podstawie badanej próby kontrolnej oceniono, że we wszystkich przypadkach przeglądanie danych miało związek z wykonywaniem czynności służbowych, z zachowaniem zasad bezpieczeństwa informacji.

2. CRCM

Badanie przeprowadzono na próbie 10 podmiotów przeglądanych przez pięciu pracowników[31] .
Na podstawie złożonych wyjaśnień potwierdzonych stosownymi dokumentami ustalono, co następuje.

- ✓ pracownik E. L. – przeglądała dane 2 podmiotów, udokumentowała związek przeglądania danych z realizowanymi czynnościami służbowymi.
- ✓ pracownik P. P. – przeglądała dane 4 podmiotów, udokumentowała związek przeglądania danych z realizowanymi czynnościami służbowymi.
- ✓ pracownik B. K. – przeglądała dane 1 podmiotu, udokumentowała związek przeglądania danych z realizowanymi czynnościami służbowymi.
- ✓ pracownik M. L. – przeglądała dane 2 podmiotów. W jednym przypadku udokumentowała związek przeglądania danych z realizowanymi czynnościami służbowymi. W drugim przypadku dokonała sprawdzenia na telefoniczny wniosek pracownika komórki SEE. W związku z tym, że nie było możliwości ustalenia miejsca pobytu podatnika, komórka SEE zbierała informacje o majątku podatnika do uzasadnienia umorzenia postępowania egzekucyjnego.

  Z wyjaśnień NUS wynika, że w kontrolowanym okresie pracownicy komórki SEE nie posiadali uprawnień do CRCM, stąd wniosek do pracownika innej komórki. Pracownikom SEE nadano uprawnienia do aplikacji 13 września 2023 r.

[28] Pismo (…) z 18 sierpnia 2023 r. z załącznikami,
[29] Pismo (…) z 22 sierpnia 2023 r. z załącznikami,
[30] M.L., P.P., B.K.,
[31] K.W. (kierownik SKA-1), E.L., M.L., P.P., B.K.,

(dowód: pismo NUS – SZD, UNP:2201-23-132796)

Uwagi kontrolerów

Zgodnie z zasadą przywilejów koniecznych, określoną w Polityce Bezpieczeństwa Informacji w Izbie Administracji Skarbowej w Gdańsku[32], każdy pracownik posiada prawo dostępu do informacji ograniczone wyłącznie do tych, które są konieczne do wykonywania powierzonych mu zadań. Stosowanie powyższej zasady oznacza ograniczenie ról i uprawnień użytkownikom systemu wyłącznie do koniecznych, w celu prawidłowej realizacji zadań służbowych oraz właściwego i zgodnego z przeznaczeniem wykorzystywania systemów teleinformatycznych.

Pozyskiwanie danych na potrzeby nie związane z czynnościami wykonywanymi przez pracownika narusza zasady dostępności i poufności i stanowi incydent bezpieczeństwa informacji.

Zgodnie z zasadami odpowiedzialności, określonymi w Polityce Ochrony Danych Osobowych IAS w Gdańsku, osobami odpowiedzialnymi za naruszenie powyższych zasad są wszyscy użytkownicy/pracownicy oraz bezpośredni przełożony.

- ✓ kierownik SKA-1 – przeglądał dane 1 podmiotu. W CRCM dokonał wyszukania i przekazał telefonicznie podatnikowi informacje dot. dat wydania postanowień Sądu Rejonowego w Chojnicach stwierdzających nabycie spadku po zmarłej matce podatnika.
  Według wyjaśnień NUS, kierownik SKA-1 dokonał tej czynności na telefoniczny wniosek podatnika, a podatnik jest mu znany osobiście. Dotyczyło to czynności służbowych dokonywanych na wniosek podatnika.

(dowód: pismo NUS – SZD, UNP:2201-23-132796)

Uwagi kontrolerów

Nie uznano wyjaśnień. Aplikacja CRCM służy obsłudze zadań związanych z odnotowywaniem czynności majątkowych na potrzeby realizowanych czynności i postępowań. Baza danych w CRCM nie może być źródłem informacji dla innych celów. Istnieją przesłanki wskazujące, że przeglądanie danych nie miało związku z realizowanymi czynnościami służbowymi, dodatkowo dotyczyło to osoby znanej osobiście osobie przeglądającej dane w CRCM. Naczelnik nie przedstawił żadnych dowodów potwierdzających prowadzenie czynności służbowych wobec podatnika, którego dotyczyło wyszukanie.

Przeglądanie danych niezwiązanych z realizowanymi czynnościami służbowymi stanowi nieprawidłowość. Nieuprawniony dostęp do danych podmiotu w CRCM stanowi potencjalny incydent bezpieczeństwa informacji.

Zgodnie z zasadami odpowiedzialności, określonymi w Polityce Ochrony Danych Osobowych IAS w Gdańsku, osobami odpowiedzialnymi za naruszenie powyższych zasad są wszyscy użytkownicy/pracownicy oraz bezpośredni przełożony.

[32] Załącznik do zarządzenia nr (…) Dyrektora Izby Administracji Skarbowej w Gdańsku z dnia 25 maja 2018 r. w sprawie ustanowienia Systemu Zarządzania Bezpieczeństwem Informacji w Izbie Administracji Skarbowej w Gdańsku

Ustalenia:
Na podstawie badanej próby kontrolnej pozytywnie oceniono wykorzystanie systemu SeRCe – we wszystkich przypadkach przeglądanie danych miało związek z wykonywaniem czynności służbowych, z zachowaniem zasad bezpieczeństwa informacji.

Wykorzystywanie aplikacji CRCM było, co do zasady, prawidłowe. Tylko w 2 przypadkach na 10 badanych stwierdzono następujące nieprawidłowości: w 1 przypadku wystąpiło naruszenie zasad dostępności i poufności – pracownik dokonał sprawdzenia w aplikacji dla innego pracownika, w 1 przypadku pracownik wykorzystał dane z systemu niezgodnie z przeznaczeniem. Opisane nieprawidłowości stanowią potencjalny incydent bezpieczeństwa informacji.

Ogółem na 25 badanych wyszukiwań w systemach SeRCe i CRCM, w 23 przypadkach wykazano związek z realizowanymi czynnościami służbowymi (92% badanej populacji)

Pozytywnie oceniono działania podjęte przez NUS w trakcie kontroli polegające na nadaniu uprawnień do CRCM pracownikom komórki SEE. Posiadanie uprawnień niezbędnych do wykonywania zadań umożliwi przestrzeganie zasad dostępności i poufności.

Osoby odpowiedzialne za stwierdzone nieprawidłowości:

- ✓ Pani M. L. w zakresie braku związku przeglądania danych w systemie CRCM z realizowanymi czynnościami służbowymi (naruszenie zasad dostępności i poufności),
- ✓ Pan K. W. w zakresie nieuprawnionego przeglądania danych w systemie CRCM oraz w zakresie braku nadzoru nad czynnościami pracownika w systemie CRCM,
- ✓ Zastępca Naczelnika Pani Honorata Szwak w zakresie nadzoru sprawowanego nad Pionem Kontroli i Orzecznictwa .

Ocena cząstkowa:
Działalność Urzędu Skarbowego w Tczewie należy ocenić ***pozytywnie z nieprawidłowościami.***

Stan prawny:
Jak w zagadnieniu pierwszym.

Zagadnienie <u>trzecie</u> z zakresu badania Nadzór nad prawidłowością wykorzystania danych z systemów informatycznych w ramach kontroli funkcjonalnej

Opis stanu faktycznego:
Kwestie regulujące zasady sprawowania kontroli funkcjonalnej zostały określone w Instrukcji dot. szczegółowych zasad przeprowadzania kontroli funkcjonalnej sprawowanej w ramach nadzoru służbowego przez osoby zajmujące kierownicze stanowiska w Izbie Administracji Skarbowej w Gdańsku, urzędach skarbowych woj. pomorskiego i pomorskim urzędzie celno-skarbowym w Gdyni stanowiącą załącznik do zarządzenia Dyrektora Izby Administracji Skarbowej w Gdańsku[33]. Kontrola funkcjonalna sprawowana jest w oparciu o Plan Kontroli funkcjonalnej, który określa szczegółowy

[33] W badanym okresie obowiązywały instrukcje wprowadzone zarządzeniami Dyrektora IAS w Gdańsku :
1. nr (…) z dnia 3 grudnia 2019 r.,
2. nr (…) 7/2023 z dnia 26 stycznia 2023 r.

zakres oraz częstotliwość kontroli funkcjonalnej. Plan kontroli przygotowują osoby zobowiązane do jej sprawowania i przedstawiają do akceptacji Naczelnikowi lub jego Zastępcy.
Zgodnie z treścią Instrukcji, kontrola funkcjonalna powinna uwzględniać specyfikę zadań realizowanych przez daną komórkę organizacyjną i koncentrować się w szczególności na ochronie danych osobowych[34].

Naczelnik Urzędu oświadczył, że zagadnienia z kontrolowanego obszaru nie zostały ujęte w planie kontroli funkcjonalnej na 2023 rok. Wskazał, że w grudniu 2022 roku oraz w II półroczu 2023 roku zostały przeprowadzone doraźne (pozaplanowe) kontrole funkcjonalne dotyczące zabezpieczenia dokumentów, informacji i danych osobowych. W grudniu 2022 r. przeprowadzono łącznie 9 kontroli doraźnych, podczas których nie stwierdzono nieprawidłowości. Natomiast w II półroczu 2023 r. łącznie przeprowadzono 6 kontroli, z czego w 3 stwierdzono nieprawidłowości, w następstwie czego wydano zalecenia pokontrolne i je zrealizowano.

Ponadto, w II półroczu 2023 r. przewidziane są doraźne kontrole funkcjonalne w zakresie wykorzystania przez pracowników systemów informatycznych do celów służbowych, polegające na zwróceniu się do Departamentu Poboru Podatków Ministerstwa Finansów oraz Referatu Kontroli Podatkowej, Kontroli Celno – Skarbowej i Nadzoru nad Czynnościami Sprawdzającymi w Izbie Administracji Skarbowej w Gdańsku z wnioskiem o przesłanie stosownych raportów.

Nadzór nad ochroną danych osobowych w systemach informatycznych sprawowany był przez kierowników/Zastępcę Naczelnika/ Naczelnika poprzez zlecanie obowiązków wymagających dostępu do systemów wyłącznie pracownikom posiadającym stosowne uprawnienia, uzasadnione zakresem wykonywanych przez nich obowiązków. Pracownicy byli na bieżąco instruowani (poprzez cykliczne spotkania Naczelnika ze wszystkimi pracownikami, cotygodniowe spotkania Naczelnika i Zastępcy Naczelnika z kierownikami) w zakresie obowiązku przestrzegania zasad ochrony danych osobowych - m.in. w zakresie zakazu dostępu do tych danych osobom nieupoważnionym (np. w postaci udzielania informacji telefonicznej); obowiązku wylogowywania się z systemów w przypadku chwilowego opuszczenia stanowiska pracy; zakazu udostępniania danych umożliwiających zalogowanie się do tych systemów; ustawienia monitorów ekranowych w sposób wykluczający zapoznanie się z wyświetlanymi na nich informacjami przez osoby nieuprawnione itp. Pracownicy zapoznani zostali z obowiązującymi zasadami ochrony danych osobowych poprzez polecenie realizacji szkoleń udostępnionych na resortowych platformach szkoleniowych. Każdorazowo redagowane przez pracowników pisma wychodzące na zewnątrz US przedstawiane były do akceptacji kierownika/Zastępcy naczelnika/Naczelnika w systemie SZD celem wyeliminowania przypadków udostępnienia informacji o danych podatników/płatników osobom/podmiotom nieuprawnionym.

(dowód: pismo NUS – SZD, UNP:2201-23-116943)

Uwagi kontrolerów

Zgodnie z zasadami ww. zarządzeń Dyrektora IAS w Gdańsku, osoby zajmujące stanowiska kierownicze, winny uwzględnić w planach kontroli funkcjonalniej w szczególności ochronę danych osobowych. W trakcie kontroli ustalono, że obszar ten nie został ujęty w planach kontroli, prawidłowość

[34] §(…)

wykorzystania danych z systemów informatycznych nie była również objęta nadzorem w ramach doraźnych kontroli funkcjonalnych.
Pozytywnie należy ocenić przeprowadzane cyklicznie przez Naczelnika doraźne (pozaplanowe) kontrole funkcjonalne w grudniu 2022 roku oraz w II półroczu 2023 roku dotyczące zabezpieczenia dokumentów, informacji i danych osobowy oraz przewidziane w II półroczu doraźne (pozaplanowe) kontrole funkcjonalne w zakresie wykorzystania przez pracowników systemów informatycznych do celów służbowych.

Formy nadzoru opisane w wyjaśnieniach są nie wystarczające, z uwagi na stwierdzone, opisane w zagadnieniu drugim nieprawidłowości w zakresie naruszenia zasad dostępności i poufności oraz wykorzystania danych z systemu niezgodnie z przeznaczeniem.

Ustalenia:
W działalności kontrolowanej jednostki w przedstawionym powyżej stwierdzono następujące nieprawidłowości:
Osoby zajmujące stanowiska kierownicze nie uwzględniły w planach kontroli funkcjonalnej w 2023 ochrony danych osobowych, a kontrole doraźne nie obejmowały prawidłowości wykorzystania danych z systemów informatycznych.

Ocena cząstkowa:
Działalność Urzędu Skarbowego w Chojnicach należy ocenić negatywnie.

Stan prawny:
- ✓ Zarządzenie nr (…) Dyrektora Izby Administracji Skarbowej w Gdańsku z dnia 3 grudnia 2019 r. w sprawie zasad przeprowadzania kontroli funkcjonalnej sprawowanej w ramach nadzoru służbowego przez osoby zajmujące kierownicze stanowiska w Izbie Administracji Skarbowej w Gdańsku, urzędach skarbowych woj. pomorskiego i Pomorskim Urzędzie Celno-Skarbowym w Gdyni,
- ✓ Zarządzenie nr (…) Dyrektora Izby Administracji Skarbowej w Gdańsku z dnia 26 stycznia 2023 r. w sprawie zasad przeprowadzania kontroli funkcjonalnej sprawowanej w ramach nadzoru służbowego przez osoby zajmujące kierownicze stanowiska w Izbie Administracji Skarbowej w Gdańsku, urzędach skarbowych woj. pomorskiego i Pomorskim Urzędzie Celno-Skarbowym w Gdyni.

III. Pozostałe informacje

Przedstawiając powyższe ustalenia kontroli Dyrektor Izby Administracji Skarbowej w Gdańsku poleca:
1) Wykorzystywać dane z rejestrów centralnych wyłącznie do celów związanych z wykonywanymi czynnościami służbowymi.
2) Zwiększyć nadzór nad realizacją szkoleń w wyznaczonych terminach przez pracowników oraz objąć ten obszar kontrolą funkcjonalną.
3) Realizować polecenia Dyrektora Izby Administracji Skarbowej w Gdańsku dot. zapoznania się z obowiązującymi zarządzeniami.

4) Dostosować uprawnienia pracowników w systemie CRCM do zadań określonych w zakresie uprawnień i obowiązków. Przestrzegać zasady, że uprawnienie „kierownik merytoryczny REJ" przeznaczone jest wyłącznie dla kierownika komórki oraz pracowników wyznaczonych do jego zastępowania.
5) Objąć kontrolą funkcjonalną zagadnienia związane z ochroną danych osobowych, w tym dot. zasadności przetwarzania danych za pośrednictwem systemów informatycznych, uwzględnić te zagadnienia w planach kontroli.

Zgodnie z art. 48 ustawy o kontroli w administracji rządowej od wystąpienia pokontrolnego nie przysługują środki odwoławcze.

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 wystąpienia pokontrolnego 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.

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

Gdańsk, dnia 11 października 2023 r.

Dyrektor Izby Administracji Skarbowej
w Gdańsku
Barbara Bętkowska-Cela
(podpisano kwalifikowanym podpisem elektronicznym)