



Krajowa Administracja
Skarbowa

**Izba Administracji Skarbowej
w Gdańsku**

2201-IWA.0921.7.2023

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

I. Dane identyfikacyjne kontroli

Temat kontroli:

Przestrzeganie przepisów o ochronie danych osobowych oraz tajemnicy skarbowej.

Jednostka kontrolowana:

Urząd Skarbowy w Słupsku
ul. Szczecińska 59
76-200 Słupsk

Kierownik jednostki kontrolowanej:

Pan Krzysztof Zdunek – Naczelnik US w Słupsku

Kontrolerzy:

- Sylwester Żurawski – główny ekspert skarbowy– koordynator kontroli
- Weronika Prabucka – młodszy kontroler skarbowy

działający na podstawie upoważnienia Dyrektora Izby Administracji Skarbowej nr 2201-IWA.0921.7.2023 z 22.03.2023 r.

Data rozpoczęcia i zakończenia czynności kontrolnych

- rozpoczęcie czynności kontrolnych - 22.03.2023 r.
- zakończenie czynności kontrolnych – 12.05.2023 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 - poz. 1

Okres objęty kontrolą: od 01.01.2022 r. do 28.02.2023 r.

Zakres przedmiotowy kontroli:

1. Przestrzeganie zasad bezpieczeństwa informacji.
Monitoring wizyjny (oznaczenie obszaru, klauzula informacja, przechowywanie, udostępnianie oraz usuwanie danych z monitoringu wizyjnego). Dostępność klauzuli informacyjnej dot. przetwarzania danych.
2. Wydawanie i unieważnianie upoważnień, szkolenia wstępne, prowadzenie szkoleń w zakresie ochrony danych.
3. Uprawnienia do systemów informatycznych.
4. Ochrona informacji - tajemnicy skarbowej.

II. Ocena kontrolowanej działalności

Ocena ogólna:

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

Uzasadnienie oceny ogólnej:

ocena dotyczy działań Naczelnika zrealizowanych w okresie od 01.01.2022 r. do 28.02.2023 r. w aspekcie:

- Przestrzegania zasad bezpieczeństwa informacji, w tym monitoringu wizyjnego (oznaczenie obszaru, klauzula informacja, przechowywanie, udostępnianie oraz usuwanie danych z monitoringu wizyjnego). Dostępności klauzuli informacyjnej dot. przetwarzania danych.
- Wydawania i unieważniania upoważnień, szkoleń wstępnych, prowadzenia szkoleń w zakresie ochrony danych.
- Uprawnień do systemów informatycznych.
- Ochrony informacji - tajemnicy skarbowej.

Szczegółowe uzasadnienie oceny stanowią poniższe uwagi i oceny częściowe dotyczące kontrolowanych zagadnień.

III. Opis ustalonego stanu faktycznego

Zagadnienie pierwsze z zakresu badania:

Przestrzeganie zasad bezpieczeństwa informacji. Monitoring wizyjny (oznaczenie obszaru, klauzula informacja, przechowywanie, udostępnianie oraz usuwanie danych z monitoringu wizyjnego). Dostępność klauzuli informacyjnej dot. przetwarzania danych.

Stan prawny:

Regulacje zewnętrzne

1. 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);
2. Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (t.j. Dz. U. z 2019 r. poz. 1781);
3. Ustawa z dnia 16 listopada 2016 o Krajowej Administracji Skarbowej (Dz. U. z 2022 r., poz. 813 ze zm.);
4. Ustawa z dnia 29 sierpnia 1997 r. Ordynacja podatkowa (t.j. Dz. U. z 2022 r. poz. 2651 ze zm.);

Regulacje wewnętrzne:

1. Zarządzenie Dyrektora Izby Administracji Skarbowej w Gdańsku w sprawie wprowadzenia Polityki Ochrony Danych Osobowych (45/2020 z 16 czerwca 2020 r.);

2. Zarządzenie Ministra Finansów, Funduszy i Polityki Regionalnej z dnia 29 grudnia 2020 r. w sprawie wprowadzenia Polityki Ochrony Danych Osobowych;
3. Zarządzenie nr 120/2021 Dyrektora Izby Administracji Skarbowej w Gdańsku z dnia 30 września 2021 r. w sprawie nadania regulaminu organizacyjnego Izbie Administracji Skarbowej w Gdańsku;
4. Zarządzenie nr 3/2022 Dyrektora Izby Administracji Skarbowej w Gdańsku z dnia 10 stycznia 2022 r. w sprawie nadania regulaminu organizacyjnego Izbie Administracji Skarbowej w Gdańsku;
5. Zarządzenie nr 61/2022 Dyrektora Izby Administracji Skarbowej w Gdańsku z dnia 9 maja 2022 r. w sprawie zmiany regulaminu organizacyjnego Izby Administracji Skarbowej w Gdańsku;
6. Zarządzenie nr 119/2022 Dyrektora Izby Administracji Skarbowej w Gdańsku z dnia 29 listopada 2022 r. w sprawie nadania regulaminu organizacyjnego Izbie Administracji Skarbowej w Gdańsku;
7. Upoważnienie nr 254/2021 z dnia 13.08.2021 r. do wykonywania zadań administratora danych w Urzędzie Skarbowym w Słupsku;
8. Zarządzenia Dyrektora Izby Administracji Skarbowej w Gdańsku w sprawie wprowadzenia instrukcji „Postępowanie z informacjami stanowiącymi tajemnicę skarbową w Izbie Administracji Skarbowej w Gdańsku”;
9. Decyzja nr 323/2022 Dyrektora Izby Administracji Skarbowej w Gdańsku z dnia 29 września 2022 r. w sprawie powołania Zespołu Reagowania na Incydenty Bezpieczeństwa w Izbie Administracji Skarbowej w Gdańsku;
10. Decyzja nr 143/2020 Dyrektora izby Administracji Skarbowej w Gdańsku z dnia 21 lipca 2020 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;
11. Decyzja nr 62/2022 Dyrektora izby Administracji Skarbowej w Gdańsku z dnia 2 marca 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;
12. Decyzja nr 209/2022 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;
13. Pismo Dyrektora Izby Administracji Skarbowej w Gdańsku nr 2201-IWD.0140.15.2020.1 z dnia 21.10.2020 r.;
14. Pismo Dyrektora Izby Administracji Skarbowej w Gdańsku nr 2201-IWD.0140.3.2021.1 z dnia 08.02.2021 r.;
15. Pismo Dyrektora Izby Administracji Skarbowej w Gdańsku nr 2201-IWD.0140.10.2021.1 z dnia 25.03.2021 r.;
16. Pismo Dyrektora Izby Administracji Skarbowej w Gdańsku nr 2201-IWD.0140.13.2021.2 z dnia 30.04.2021 r.;
17. Pismo Dyrektora Izby Administracji Skarbowej w Gdańsku nr 2201-IWD.0140.15.2021 z dnia 13.05.2021 r.;

18. Pismo Dyrektora Izby Administracji Skarbowej w Gdańsku nr 2201-IWD-0140.2.2022.2 z dnia 12.01.2022 r.;
19. Pismo Dyrektora Izby Administracji Skarbowej w Gdańsku nr 2201-IWD-0140.11.2022.3 z dnia 30.03.2022 r.;
20. Pismo Dyrektora Izby Administracji Skarbowej w Gdańsku nr 2201-IWD-0140.20.2022 z dnia 31.05.2022 r.;
21. Pismo Dyrektora Izby Administracji Skarbowej w Gdańsku nr 2201-IWD.0140.26.2022 z dnia 22.07.2022 r.;
22. Pismo Dyrektora Izby Administracji Skarbowej w Gdańsku nr 2201-IWD-0140.1.2023 z dnia 02.01.2023 r.;
23. Regulaminy organizacyjne Urzędu Skarbowego w Słupsku, obowiązujące w kontrolowanym okresie.

Opis stanu faktycznego:

W oparciu o obowiązujące ówczesnie Regulaminy organizacyjne Urzędu Skarbowego w Słupsku kontrolujący ustalili, że realizacja zadań w zakresie nadzoru służbowego nad obszarem objętym kontrolą sprawowali:

- Pan Cezary Lewiński – Naczelnik US w Słupsku (01.09.2016 – 15.08.2021)
- Pan Krzysztof Zdunek – Naczelnik US w Słupsku (od 16.08.2021)

[Dowód: Q-asystent]

Administratorem danych osobowych, zgodnie z art. 232 ustawy z dnia 16 listopada 2016 r., przepisy wprowadzające ustawę o KAS, w IAS w Gdańsku jest Dyrektor.

Na podstawie upoważnienia nr 254/2021 z 13 sierpnia 2021, do wykonywania zadań administratora danych w Urzędzie Skarbowym w Słupsku dla danych, których administratorem jest Dyrektor Izby Administracji Skarbowej w Gdańsku, w zakresie:

- nadzoru nad bezpieczeństwem przetwarzania danych osobowych,
- udzielania i odwoływania upoważnień do przetwarzania danych osobowych,
- zatwierdzania uprawnień do systemów informatycznych,

był Pan Krzysztof Zdunek – od 16.08.2021.

[Dowód: Q-asystent]

Na podstawie Decyzji nr 254/2021 z dnia 13 sierpnia 2021 r., 62/2022 z dnia 2 marca 2022 r. oraz 209/2022 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 (i wcześniejszych), w Urzędzie Skarbowym w Słupsku osobą odpowiedzialną za realizację zadań z zakresu ochrony danych osobowych jest pan **W.P.**, główny ekspert skarbowy, Trzeci Referat Czynności Analitycznych i Sprawdzających.

Do zadań pracownika należy w szczególności:

- a) organizacja i prowadzenie szkoleń wstępnych z zakresu ochrony danych osobowych (w Urzędach dotyczy praktykantów, stażystów, aplikantów, wolontariuszy, pracowników ochrony, osób zatrudnionych na umowę zlecenie, oraz pracowników świadczących usługi);

- b) weryfikacja upoważnień oraz szkolenie pracowników powracających do pracy po długotrwałej nieobecności;
- c) prowadzenie ewidencji szkoleń i ich uczestników;
- d) sporządzanie upoważnień do przetwarzania danych osobowych i przedkładanie ich do podpisu administratorowi lub osobie przez niego upoważnionej (w Urzędach dotyczy praktykantów, stażystów, aplikantów, wolontariuszy, pracowników ochrony, osób zatrudnionych na umowę zlecenie oraz pracowników świadczących usługi);
- e) prowadzenie ewidencji osób upoważnionych do przetwarzania danych osobowych;
- f) weryfikacja wniosków o nadanie uprawnień do systemów informatycznych pod względem zgodności z upoważnieniem do przetwarzania danych osobowych, a w przypadku akceptacji Zgody na wnoszenie komputera poza miejsce pracy – dodatkowo weryfikacja, czy został załączony podpisany wniosek.
- g) współpraca z Inspektorem Ochrony Danych Izby Administracji Skarbowej w Gdańsku w zakresie realizacji zadań wynikających z przepisów o ochronie danych osobowych.

Zgodnie z Polityką Ochrony Danych Osobowych w IAS Gdańsk (dalej zwanej Polityką), kierujący komórką organizacyjną/samodzielnym stanowiskiem odpowiada za nadzór nad zapewnieniem prawidłowego działania zabezpieczeń organizacyjnych integralności, poufności, rozliczalności w zakresie stosownym do powierzonych im zasobów (aktywów). Kierujący komórką bezpieczeństwa i ochrony informacji odpowiedzialny jest dodatkowo za nadzór nad ochroną fizyczną przetwarzanych danych osobowych.

W Urzędzie Skarbowym w Słupsku funkcjonują, zgodnie z Regulaminem organizacyjnym, następujące komórki organizacyjne, na których czele stoją kierownicy działów/referatów/kierujący:

- SOB1 – E.K.;
- SOB2 – B.C.;
- SKI – A.M.;
- SER – A.P.;
- SKA-1 – T.N.;
- SKA-2 – A.B.;
- SKA-3 – W.S.;
- SEE – P.G.;
- SWW – A.W.;
- SEW – I.U.;
- SKP – L.Ł.;
- SPV-1 – A.S.;
- SPV-2 – A.M2;
- SPM – M.B.;
- SPA – A.L..

Wszyscy kierownicy (oprócz Pani A.W.) złożyli oświadczenia w których opisali jak sprawują nadzór ws. ochrony danych osobowych oraz informacji niejawnych. Zaznaczyli m. in., że na bieżąco informują podległych pracowników o zasadach bezpieczeństwa danych osobowych, a w szczególności czystego biurka, ochronie fizycznej dokumentów (zamykanie w szafach), prawidłowego niszczenia

dokumentów, właściwego adresowania korespondencji (papierowej i elektronicznej). Wszyscy przekazują informacje z narad kierownictwa poświęconych tej tematyce.

[Dowód: akta kontroli, str. nr 85-87, 139-154]

Polityka określa obowiązki poszczególnych pracowników – użytkowników. Użytkownik jest kluczowym elementem struktury zarządzania bezpieczeństwem danych osobowych. Jest on odpowiedzialny za przestrzeganie zasad ochrony danych osobowych, zabezpieczenie danych osobowych przed ich udostępnieniem osobom nieupoważnionym, przetwarzaniem z naruszeniem przepisów prawa, zabranieniem przez osobę nieuprawnioną, uszkodzeniem lub zniszczeniem. Jego obowiązkiem jest również ochrona własnych kont i haseł umożliwiających dostęp do danych osobowych. Lista pracowników świadczących pracę w US Słupsku jest dowodem w aktach kontroli.

[Dowód: akta kontroli, str. nr 60-64]

W kontrolowanym okresie nie przeprowadzono kontroli funkcjonalnych.

Naczelnik złożył oświadczenie, w którym opisał swoje działania ws. ochrony danych osobowych. Są to m. in. polecenie sprawdzenia przez IOD w US w Słupsku stanu zabezpieczeń dokumentów w pomieszczeniach, a także omówienie w dniu 27.10.2021 r., w obecności radcy prawnego, zasad dotyczących ochrony informacji stanowiących tajemnicę skarbową oraz ochrony informacji stanowiących dane osobowe, przypadki naruszeń ochrony tajemnicy skarbowej i ochrony danych osobowych, sankcje karne związane z naruszeniem zasad ochrony danych, odpowiedzialność funkcjonariusza publicznego wynikającą z art. 231 Kodeksu karnego.

[Dowód: akta kontroli, str. nr 85-87, 145]

W Urzędzie nie wprowadzono procedur wewnętrznych dotyczących kontrolowanego obszaru.

[Dowód: Q - asystent]

Kontrola stosowania środków bezpieczeństwa fizycznego:

Zasada uprawnionego dostępu – każdy pracownik przeszedł szkolenie z zasad ochrony informacji oraz spełnia kryteria dopuszczenia do informacji.

Zasada obecności koniecznej – prawo przebywania w określonych miejscach mają tylko osoby upoważnione.

Kontrolujący stwierdzili na podstawie oględzin i dodatkowych wyjaśnień Naczelnika:

(...)

[Dowód: akta kontroli, str. nr 633-634]

Brak uwag.

Zasady dostępu do kluczy.

Polityka dostępu do kluczy jest środkiem organizacyjnym kontroli dostępu. Polega na rejestrowaniu faktu pobierania i zdawania kluczy do chronionego pomieszczenia. Środek ten zapewnia zabezpieczenie danych osobowych od strony rozliczalności dostępu, pomagając w ustaleniu osób odpowiedzialnych za działania związane z naruszeniem bezpieczeństwa. (...)

Brak uwag.

[Dowód: akta kontroli, str. nr 324]

Ochrona fizyczna dokumentów

Za ochronę fizyczną dokumentów zawierających dane osobowe odpowiedzialni są kierujący komórkami Izby jako właściciele aktywów lub administratorzy informacji, a także ich podwładni, którym wydano formalne upoważnienie do przetwarzania danych osobowych. W szczególności odpowiedzialność za bezpieczeństwo dokumentów ponoszą pracownicy, którym powierzono informacje na zasadach wiedzy uzasadnionej.

Osoby wskazane wyżej są odpowiedzialne za zapewnienie poufności dokumentów oraz zawartych w nich informacji, a więc za niedopuszczenie, aby z informacjami zapoznali się osoby nieupoważnione. Dane osobowe oraz inne informacje powinny być przechowywane **w zamykanych szafach**, co zapewnia zabezpieczenie danych osobowych od strony poufności i integralności.

Kontrolujący dokonali oględzin 20 pomieszczeń (23 % pomieszczeń ogółem), w których zakończono już pracę. W pokoju nr (...) stwierdzono, że jedna z szaf była otwarta (nieodmknięta). Znajdowały się w niej dokumenty zawierające chronione dane. W pozostałych skontrolowanych pomieszczeniach naruszenia zasady ochrony fizycznej dokumentów nie stwierdzono.

[Dowód: akta kontroli, str. nr 47-51]

Zasada czystego biurka

Niepozostawianie dokumentów i innych nośników informacji na stanowisku pracy (biurku) podczas swojej nieobecności jest środkiem fizycznej ochrony informacji wynikającym z zasady „czystego biurka”. Zapewnienie czystego biurka polega na tym, że dane osobowe nie będą dostępne osobom nieuprawnionym do ich przetwarzania. Osobami nieuprawnionymi są zarówno osoby nieposiadające upoważnienia do przetwarzania danych osobowych, jak też posiadające takie upoważnienie, ale nieposiadające obowiązku ich przetwarzania. Wyłączenie tych osób spośród odbiorców informacji wynika z zasady wiedzy uzasadnionej. W przypadku osób posiadających formalne upoważnienie do przetwarzania danych osobowych brak uzasadnienia służbowego do zapoznania się przez nie z konkretnymi danymi osobowymi uzasadnia ochronę przed nimi dokumentów zawierających konkretne informacje.

W przypadku użytkowania dokumentów lub nośników (aktywów) poza miejscem pracy na pracowniku ciąży obowiązek zapewnienia poufności i integralności informacji.

Zasada czystego biurka, jako środek ochrony zapewnia zabezpieczenie danych osobowych od strony poufności i integralności.

Kontrolujący dokonali oględzin 20 pomieszczeń (23% pomieszczeń ogółem), w których zakończono już pracę. W pokoju nr (...) na biurku znajdowały się pisma zawierające dane osobowe. W pozostałych pokojach nieprawidłowości nie stwierdzono.

[Dowód: akta kontroli, str. nr 47-51]

Zasada czystego ekranu

Ekran komputera, z którego nie można łatwo odczytać informacji, jest organizacyjnym środkiem ochrony wynikającym z zasady „czystego ekranu”. Podobnie jak w przypadku biurka, na którym mogą znajdować się dokumenty zawierające dane osobowe, na ekranie komputera osoba nieuprawniona może odczytać treść wyświetlanych aktualnie dokumentów elektronicznych. Zasada czystego ekranu, jako środek ochrony zapewnia zabezpieczenie danych osobowych od strony poufności.

Kontrolujący sprawdzili przestrzeganie tej zasady w pok. (...) i (...) w ten sposób, że poproszono osoby pracujące przy komputerze o chwilowe odejście od stanowiska pracy. W obydwu przypadkach pracownicy prawidłowo zablokowali pracę komputera (włączony wygaszacz ekranu).

[Dowód: akta kontroli, str. nr 47-51]

Zasady czystej tablicy, czystego kosza i czystych drukarek.

Na tablicach, np. korkowych nie mogą znajdować się dokumenty zawierające dane chronione.

Zasada czystego kosza polega na niszczeniu dokumentów, na których znajdują się poufne informacje, w taki sposób, aby ich odczytanie było niemożliwe. Do tego celu najlepiej używać niszczarki. Zasada ta mówi także, aby nie wyrzucać dokumentów do kosza obok biurka.

Zasada czystych drukarek w skrócie mówi, że niedozwolone jest pozostawianie urządzenia w trakcie drukowania/skanowania/kopiowania bez nadzoru, jeżeli materiały znajdujące się w urządzeniu zawierają dane osobowe. Niedozwolone jest również pozostawianie na ekranie urządzenia wielofunkcyjnego dokumentów zawierających dane osobowe. W okolicy urządzenia nie mogą znajdować się pozostawione dokumenty z danymi (na stołach, krzesłach, parapetach etc.)

Skontrolowano 20 pomieszczeń (23% ogółem). Worki ze ścinkami przechowywane są w piwnicy budynku, do której dostęp dla osób postronnych jest ograniczony. Naruszeń w/w zasad nie stwierdzono.

[Dowód; akta kontroli, str. nr 47-51, 324]

Zestawienie skontrolowanych pomieszczeń.

Lp.	Komórka	Nr pokoju	UWAGI
1.	SKA-1	(...)	Nie stwierdzono nieprawidłowości
2.	SKA-1	(...)	Nie stwierdzono nieprawidłowości
3.	SKA-1	(...)	Nie stwierdzono nieprawidłowości
4.	SKA-3	(...)	Nie stwierdzono nieprawidłowości
5.	SKA-3	(...)	Nie stwierdzono nieprawidłowości
6.	SKA-3	(...)	Nie stwierdzono nieprawidłowości
7.	SOB2	(...)	Nie stwierdzono nieprawidłowości
8.	SKP	(...)	Nie stwierdzono nieprawidłowości
9.	SKP	(...)	Nie stwierdzono nieprawidłowości
10.	SPV-1	(...)	Nie stwierdzono nieprawidłowości
11.	SPV-1	(...)	Nie stwierdzono nieprawidłowości
12.	SEW	(...)	Pisma z danymi osobowymi na biurku
13.	SEW	(...)	Nie stwierdzono nieprawidłowości

Lp.	Komórka	Nr pokoju	UWAGI
14.	SEW	(...)	Nie stwierdzono nieprawidłowości
15.	SPV-2	(...)	Nie stwierdzono nieprawidłowości
16.	SPV-2, SPA	(...)	Nie stwierdzono nieprawidłowości
17.	SPV-2	(...)	Otwarta szafa z dokumentami zawierającymi dane osobowe
18.	SPV-2	(...)	Nie stwierdzono nieprawidłowości
19.	SOB1	(...)	Nie stwierdzono nieprawidłowości
20.	SOB1	(...)	Nie stwierdzono nieprawidłowości

Wysyłka korespondencji

Gromadzone dane osobowe powinny być adekwatne, stosowne i ograniczone do tego, co niezbędne do celów, dla których są one przetwarzane. Wymaga to w szczególności ograniczenia ilości gromadzonych danych do ścisłego minimum. Dane osobowe powinny być przetwarzane tylko w przypadkach, gdy celu przetwarzania nie można w rozsądny sposób osiągnąć innymi sposobami. Jest to zasada minimalizacji danych osobowych, opisana w art. 5 ust. 1 lit. c RODO.

DIAS w pismach nadzorczych:

1. 2201-IWD.0140.15.2020.1 z 21.10.2020 r.
2. 2201-IWD.0140.10.2021.1 z 25.03.2021 r.,

polecił zachowanie szczególnej uwagi przy umieszczaniu w danych adresowych, a w szczególności nie umieszczaniu nr PESEL, lub umożliwienie osobom trzecim zapoznania się przez „okienko adresowe” na kopercie z tym numerem ew. z serią i nr. dokumentu tożsamości, nr. rachunku bankowego etc. Naruszenie tych zasad powoduje wysokie ryzyko dla praw i wolności osób, których dane zostały ujawnione.

Kontrolujący sprawdzili korespondencję przygotowaną do wysyłki (121/250 listów). W żadnym przypadku nie stwierdzono naruszenia zasad o których mowa wyżej.

Brak uwag.

[Dowód: akta kontroli, str. nr 324]

Monitoring wizyjny (oznaczenie obszaru, klauzula informacja, przechowywanie, udostępnianie oraz usuwanie danych z monitoringu wizyjnego). Dostępność klauzuli informacyjnej dot. przetwarzania danych.

Głównym celem Systemu Telewizji Przemysłowej jest zapewnienie bezpieczeństwa pracowników i ochrony mienia, nie mniej pośrednio wspiera on kontrolę obecności osób w obszarze monitorowanym przez kamery systemu. Stosuje się go w celu monitorowania obszarów, nad którymi sprawowana jest kontrola. Środek ten, nie ogranicza dostępu, ale umożliwia zabezpieczenie danych osobowych od strony rozliczalności, pomagając w ustaleniu osób odpowiedzialnych za działania związane z naruszeniem bezpieczeństwa.

Kontrolujący sprawdzili:

1. Klauzule informacyjne.

Na drzwiach budynku, tablicach informacyjnych oraz pod wszystkimi kamerami umieszczono informację, że obiekt jest monitorowany. Zamieszczono również klauzulę informacyjną z zasadami RODO.

Brak uwag.

[Dowód: akta kontroli, str. 324]

2. Przechowywanie nagrań oraz ich usuwanie,

Zgodnie z oświadczeniem Naczelnika, nagrania z monitoringu nadpisywane są po 7 dniach.

Brak uwag.

[Dowód, akta kontroli, str. nr 398-402]

3. Udostępnianie nagrań z monitoringu.

W kontrolowanym okresie Naczelnik udostępnił dwa razy nagranie z CCTV. Odbędzie się to na wnioski Komendy Miejskiej Policji w (...) z 30.11.2022 r. oraz 11.01.2023 r. Nagrania przekazano na nośniku danych. Przekazująca sporządziła stosowne notatki służbowe.

Brak uwag.

[Dowód, akta kontroli, str. nr 474-481]

Zasada ochrony zewnętrznych (wymiennych) nośników danych

Zgodnie z wyjaśnieniem Naczelnika, w dyspozycji pracowników urzędu są zewnętrzne nośniki danych takie jak pendrive. Nośniki przypisane do pracownika, są zaszyfrowane hasłem i przechowywane w zamkniętej, plombowanej szafie w pokoju (...).

Brak uwag.

[Dowód, akta kontroli, str. nr 398-402, 472-473]

Ustalenia

Kontrolujący stwierdzili jedno naruszenie zasady ochrony fizycznej dokumentów (1/20 skontrolowanych pomieszczeń) oraz jedno naruszenie zasady czystego biurka (1/20 skontrolowanych pomieszczeń).

Działalność Urzędu Skarbowego w Słupsku, w zakresie przestrzegania zasad bezpieczeństwa informacji, należy ocenić **pozytywnie z uchybieniami**.

Zagadnienie drugie z zakresu badania:

Wydawanie i unieważnianie upoważnień, szkolenia wstępne, prowadzenie szkoleń w zakresie ochrony danych.

Stan prawny:

Regulacje zewnętrzne

1. 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);
2. Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (t.j. Dz. U. z 2019 r. poz. 1781);

3. Ustawa z dnia 16 listopada 2016 o Krajowej Administracji Skarbowej (Dz. U. z 2022 r., poz. 813 ze zm.);
4. Ustawa z dnia 29 sierpnia 1997 r. Ordynacja podatkowa (t.j. Dz. U. z 2022 r. poz. 2651 ze zm.);

Regulacje wewnętrzne:

1. Zarządzenie Dyrektora Izby Administracji Skarbowej w Gdańsku w sprawie wprowadzenia Polityki Ochrony Danych Osobowych (45/2020 z 16 czerwca 2020 r.);
2. Zarządzenie Ministra Finansów, Funduszy i Polityki Regionalnej z dnia 29 grudnia 2020 r. w sprawie wprowadzenia Polityki Ochrony Danych Osobowych;
3. Zarządzenie nr 120/2021 Dyrektora Izby Administracji Skarbowej w Gdańsku z dnia 30 września 2021 r. w sprawie nadania regulaminu organizacyjnego Izbie Administracji Skarbowej w Gdańsku;
4. Zarządzenie nr 3/2022 Dyrektora Izby Administracji Skarbowej w Gdańsku z dnia 10 stycznia 2022 r. w sprawie nadania regulaminu organizacyjnego Izbie Administracji Skarbowej w Gdańsku;
5. Zarządzenie nr 61/2022 Dyrektora Izby Administracji Skarbowej w Gdańsku z dnia 9 maja 2022 r. w sprawie zmiany regulaminu organizacyjnego Izby Administracji Skarbowej w Gdańsku;
6. Zarządzenie nr 119/2022 Dyrektora Izby Administracji Skarbowej w Gdańsku z dnia 29 listopada 2022 r. w sprawie nadania regulaminu organizacyjnego Izbie Administracji Skarbowej w Gdańsku;
7. Upoważnienie nr 254/2021 z dnia 13.08.2021 r. do wykonywania zadań administratora danych w Urzędzie Skarbowym w Słupsku;
8. Zarządzenia Dyrektora Izby Administracji Skarbowej w Gdańsku w sprawie wprowadzenia instrukcji „Postępowanie z informacjami stanowiącymi tajemnicę skarbową w Izbie Administracji Skarbowej w Gdańsku”;
9. Decyzja nr 323/2022 Dyrektora Izby Administracji Skarbowej w Gdańsku z dnia 29 września 2022 r. w sprawie powołania Zespołu Reagowania na Incydenty Bezpieczeństwa w Izbie Administracji Skarbowej w Gdańsku;
10. Decyzja nr 143/2020 Dyrektora izby Administracji Skarbowej w Gdańsku z dnia 21 lipca 2020 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;
11. Decyzja nr 62/2022 Dyrektora izby Administracji Skarbowej w Gdańsku z dnia 2 marca 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;
12. Decyzja nr 209/2022 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;
13. Pismo Dyrektora Izby Administracji Skarbowej w Gdańsku nr 2201-IWD.0140.15.2020.1 z dnia 21.10.2020 r.;

14. Pismo Dyrektora Izby Administracji Skarbowej w Gdańsku nr 2201-IWD.0140.3.2021.1 z dnia 08.02.2021 r.;
15. Pismo Dyrektora Izby Administracji Skarbowej w Gdańsku nr 2201-IWD.0140.10.2021.1 z dnia 25.03.2021 r.;
16. Pismo Dyrektora Izby Administracji Skarbowej w Gdańsku nr 2201-IWD.0140.13.2021.2 z dnia 30.04.2021 r.;
17. Pismo Dyrektora Izby Administracji Skarbowej w Gdańsku nr 2201-IWD.0140.15.2021 z dnia 13.05.2021 r.;
18. Pismo Dyrektora Izby Administracji Skarbowej w Gdańsku nr 2201-IWD-0140.2.2022.2 z dnia 12.01.2022 r.;
19. Pismo Dyrektora Izby Administracji Skarbowej w Gdańsku nr 2201-IWD-0140.11.2022.3 z dnia 30.03.2022 r.;
20. Pismo Dyrektora Izby Administracji Skarbowej w Gdańsku nr 2201-IWD-0140.20.2022 z dnia 31.05.2022 r.;
21. Pismo Dyrektora Izby Administracji Skarbowej w Gdańsku nr 2201-IWD.0140.26.2022 z dnia 22.07.2022 r.;
22. Pismo Dyrektora Izby Administracji Skarbowej w Gdańsku nr 2201-IWD-0140.1.2023 z dnia 02.01.2023 r.;
23. Regulaminy organizacyjne Urzędu Skarbowego w Słupsku, obowiązujące w kontrolowanym okresie.

Opis stanu faktycznego:

Podstawą działań w zakresie ochrony i jednocześnie zabezpieczeniem jest organizacja ochrony danych osobowych.

Organizacja ochrony danych dostarcza mechanizmów rozwiązywania problemów z bezpieczeństwem informacji, a także poprawiania i tworzenia odpowiednich polityk i procedur. Ustalenie odpowiedzialności za aktywa jest częścią zapewnienia, że właściwe informacje będą właściwie chronione, a przepływ informacji o ryzykach będzie właściwy.

Stan zapoznania się pracowników z dokumentacją dot. ochrony danych. Komunikacja kaskadowa wytycznych Dyrektora IAS dot. ochrony danych.

Polityki określają zasady postępowania oraz organizację działań i odpowiedzialność za ich realizację. Procedury wskazują konkretny sposób postępowania w poszczególnych przypadkach. Celem powyższej dokumentacji jest zapewnienie wytycznych i wsparcia dla działań na rzecz bezpieczeństwa informacji, zgodnie z wymaganiami biznesowymi oraz właściwymi normami prawnymi i regulacjami. Dokumentacja jest środkiem ochrony danych osobowych od strony poufności, integralności, dostępności oraz rozliczalności.

Kontrolujący sprawdzili stan zapoznania się pracowników świadczących pracę w US w Słupsku z obowiązującymi Politykami ochrony danych oraz wytycznymi DIAS w tej sprawie.

Dowodem jest zestawienie zapoznania się pracowników z dokumentem: zarządzenia Ministra Finansów, Funduszy i Polityki Regionalnej z 29 grudnia 2020 r. w sprawie Polityki Ochrony danych Osobowych (raport z aplikacji Q-asystent z 4 kwietnia 2023 r.). Wynika z niego, że na 163

zatrudnionych w US Słupsk, z dokumentem zapoznało się 151 osób, z czego 94 po rozpoczęciu kontroli. 12 osób nie zapoznało się z w/w dokumentem.

[Dowód: akta kontroli, str. nr 88-138]

Z Zarządzeniem Dyrektora Izby Administracji Skarbowej nr 45/2020 w sprawie wprowadzenia Polityki Ochrony Danych Osobowych, na 163 zatrudnionych z dokumentem zapoznało się 153 osoby, 68 zapoznało się z w/w dokumentem po wszczęciu kontroli. 10 osób nie zapoznało się (raport z aplikacji Q-asystent z 4 kwietnia 2023 r.).

[Dowód: akta kontroli, str. nr 88-138]

Wytyczne DIAS zostały przekazane wszystkim pracownikom za pomocą SZD.

[Dowód: akta kontroli, str. nr 166-230]

Upoważnienia do przetwarzania danych osobowych wydawane przez upoważnionego pracownika ds. ochrony danych osobowych.

Prowadzenie ewidencji upoważnień do przetwarzania danych osobowych.

Szkolenia wstępne.

Oświadczenia o zachowaniu poufności danych osobowych.

Do przetwarzania danych osobowych mogą być dopuszczone wyłącznie osoby zapewniające bezpieczeństwo przetwarzanych danych osobowych oraz posiadające upoważnienie do przetwarzania danych osobowych, nadane przez Administratora lub osobę przez niego upoważnioną. Osoby upoważnione do przetwarzania danych osobowych są zobowiązane do przestrzegania zasad ochrony przed nieuprawnionym dostępem (w tym fizycznym), nieuzasadnioną modyfikacją, zniszczeniem, ujawnieniem lub pozyskaniem danych oraz do prawidłowego stosowania reguł zdefiniowanych dla haseł, eksploatacji systemów informatycznych i ochrony antywirusowej. Upoważnienia są wydawane pisemnie i mogą przybierać formę aktu prawa wewnętrznego, bądź imiennego upoważniania.

Komórka obsługi kadrowej (w uzasadnionych przypadkach inna komórka organizacyjna)/ bezpośredni przełożony osoby upoważnianej przekazuje uprawnionej osobie dane osoby, której należy wystawić upoważnienie do przetwarzania danych osobowych (pracownicy, stażyści, praktykanci, wolontariusze, osoby kontrolujące, pracownicy zleceniowi, pracownicy innych jednostek organizacyjnych resortu finansów).

W Urzędzie Skarbowym w Słupsku osobą odpowiedzialną za realizację zadań z zakresu ochrony danych osobowych jest pan **W.P.**, główny ekspert skarbowy, Trzeci Referat Czynności Analitycznych i Sprawdzających. Prowadzi on ewidencję osób upoważnionych do przetwarzania danych, zgodną ze wzorem opisanym w Procedurze nadawania i odwoływania upoważnień imiennych do przetwarzania danych osobowych (załącznik do Polityki) jedynie w stosunku do części praktykantów.

Na podstawie listy zatrudnionych stażystów, aplikantów, wolontariuszy etc., otrzymanej z pionu kadr IAS, kontrolujący sprawdzili terminowość wystawiania upoważnień do przetwarzania danych oraz terminowość szkoleń w zakresie ochrony danych osobowych w/w osób.

Lp.	Imię, nazwisko (inicjały)	Stanowisko	Początek zatrudnienia	Koniec zatrudnienia	Upoważnienie do przetwarzania danych osobowych
1.	M. K.	stażysta	01.03.2022 05.10.2022	31.08.2022 30.11.2022	Upoważnienie podpisano 14 dni po rozpoczęciu stażu Upoważnienie podpisano 5 dni po rozpoczęciu stażu
2.	A. D.	stażysta	01.03.2022 21.09.2022	31.08.2022 20.03.2023	Upoważnienie podpisano 14 dni po rozpoczęciu stażu Upoważnienie podpisano 1 dzień po rozpoczęciu stażu
3.	J. B.	stażysta	01.03.2022	31.08.2022	Upoważnienie podpisano 3 dni po rozpoczęciu stażu
4.	W. I.	stażysta	01.03.2022	30.06.2022	Upoważnienie podpisano 3 dni po rozpoczęciu stażu
5.	I. L.	stażysta	01.03.2022	31.08.2022	Upoważnienie podpisano 3 dni po rozpoczęciu stażu
6.	D. F.	stażysta	01.03.2022	14.03.2022	Upoważnienie podpisano 3 dni po rozpoczęciu stażu
7.	A. M.	stażysta	01.03.2022	31.08.2022	Upoważnienie podpisano 3 dni po rozpoczęciu stażu
8.	I. K.	stażysta	01.03.2022 21.09.2022	31.08.2022 20.03.2023	Upoważnienie podpisano 14 dni po rozpoczęciu stażu Upoważnienie podpisano 5 dni po rozpoczęciu stażu
9.	K. K.	stażysta	01.03.2022	29.03.2022	Upoważnienie podpisano 3 dni po rozpoczęciu stażu
10.	W. L.	stażysta	05.10.2022	04.04.2023	Upoważnienie podpisano 5 dni po rozpoczęciu stażu

Lp.	Imię, nazwisko (inicjały)	Stanowisko	Początek zatrudnienia	Koniec zatrudnienia	Upoważnienie do przetwarzania danych osobowych
11.	A. M2	stażysta	05.10.2022	04.04.2023	Upoważnienie podpisano 5 dni po rozpoczęciu stażu
12.	A. M3	stażysta	05.10.2022	04.04.2023	Upoważnienie podpisano 5 dni po rozpoczęciu stażu
13.	J. M.	stażysta	05.10.2022	16.12.2022	Upoważnienie podpisano 5 dni po rozpoczęciu stażu
14.	E. C.	stażysta	05.10.2022	11.12.2022	Upoważnienie podpisano 5 dni po rozpoczęciu stażu
15.	A. K.	stażysta	05.10.2022	04.04.2023	Upoważnienie podpisano 5 dni po rozpoczęciu stażu
16.	W. G.	stażysta	05.10.2022	04.04.2023	Upoważnienie podpisano 5 dni po rozpoczęciu stażu
17.	P. K.	praktykant	14.03.2022	19.06.2022	BRAK
18.	M. M.	praktykant	14.03.2022	19.06.2022	BRAK
19.	W. L2	praktykant	14.03.2022	19.06.2022	BRAK
20.	R. G.	praktykant	01.07.2022	21.07.2022	BRAK
21.	J. S.	praktykant	15.11.2022	27.12.2022	Upoważnienie podpisano 2 dni po rozpoczęciu praktyki
22.	Z. G.	praktykant	15.11.2022	05.12.2022	Upoważnienie podpisano 2 dni po rozpoczęciu praktyki
23.	E. K.	praktykant	15.11.2022	05.12.2022	Upoważnienie podpisano 2 dni po rozpoczęciu praktyki
24.	H. K.	praktykant	15.11.2022	06.12.2022	Upoważnienie podpisano 2 dni po rozpoczęciu praktyki
25.	K. R.	praktykant	15.11.2022	28.11.2022	Upoważnienie podpisano 2 dni po rozpoczęciu praktyki

Czterem z w/w osób nie wystawiono upoważnienia do przetwarzania danych. Pozostałe osoby podpisały odbiór upoważnień od 1 do 14 dni po rozpoczęciu stażu/praktyki.

Wobec osób odbywających staż, praktykę, wolontariat, osób kontrolujących, pracowników zleceńowych wygaśnięcie upoważnienia następuje po upływie terminu lub zdarzenia określonego w upoważnieniu i nie wymaga odrębnego wniosku (ust. 6 przedmiotowej procedury).

Dwie z w/w osób nie zostały przeszkolone z zakresu ochrony danych osobowych na zasadach określonych w SZBI (A. D. i I. K., okres odbywania stażu: 21.09.2022 – 20.03.2023). Jedna osoba została przeszkolona dzień po rozpoczęciu stażu (A. K.), natomiast J. M. nie złożyła podpisu na oświadczeniu zapoznania się i przyjęcia do stosowania zasad zawartych w dokumentacji ochrony danych osobowych. Pozostali uczestnicy szkolenia potwierdzili zapoznanie się z obowiązującymi przepisami oraz zobowiązali się pisemnie do zachowania tajemnicy danych osobowych.

[Dowód: akta kontroli, str. nr 231-306, 311-323]

Osoby wykonujące czynności zlecone w obszarze przetwarzania danych osobowych są zobowiązane do zachowaniu poufności. Wypełniają i podpisują stosowne oświadczenie. Dotyczy to osób, których zadania, obowiązki nie wymagają przetwarzania danych osobowych na polecenie administratora danych np. personel sprzątający, wykonujący serwis urządzeń – np. drukarek, dokonujący transportu lub przemieszczenia dokumentacji, remontujący pomieszczenie, w którym przechowywane są informacje prawnie chronione.

Oświadczenia o zachowaniu poufności są środkiem ochrony danych osobowych od strony poufności.

W US w Słupsku pracuje sześciu pracowników zewnętrznych (trzech pracowników ochrony oraz trzy osoby z personelu sprzątającego). Wszystkie te osoby podpisały oświadczenie o zachowaniu poufności informacji, jednak żadne nie zostało potwierdzone datą.

[Dowód: akta kontroli, str. nr 425-432]

Kontrolujący wystąpili do VI Zastępcy Dyrektora IAS w Gdańsku z prośbą o:

- a) wykaz prac remontowych prowadzonych w pomieszczeniach urzędu,
- b) wykonanych w kontrolowanym okresie archiwizacji i brakowania dokumentów,
- c) wykonanych napraw i prac konserwacyjnych urządzeń wielofunkcyjnych w leasingu (drukarka/skaner/kopiarka).

Ponadto poprosiliśmy o informację, czy w umowie z wykonawcami w/w prac istnieje klauzula (oświadczenie) o zachowaniu poufności.

Odpowiedź brzmi:

W US w Słupsku, w 2022 i 01 – 02.2023 r. przeprowadzono następujące prace remontowe:
(...).

W urzędzie zarchiwizowano 187,20 metrów bieżących – dokumentacji kategorii B. Nie brakowano (oddawano do zniszczenia) dokumentacji w tym czasie.

Przeprowadzono prace serwisowe na urządzeniach wielofunkcyjnych – drukarka/skaner/kserokopiarka - leasingowanych od firm zewnętrznych w dniach: 22 czerwca 2022, 18 i 23 sierpnia 2022, 22 września 2022, 17 października 2022, 15 i 23 lutego 2023.

W umowie na świadczenie usługi Systemu Druku Podążającego wraz z dzierżawą i kompleksową obsługą serwisową urządzeń wielofunkcyjnych oraz oprogramowania w jednostkach Izby Administracji Skarbowej w Gdańsku (umowa leasingowa), zawarto tzw. zobowiązanie do zachowania poufności opisane w pkt. 13.3.5 Polityki Ochrony Danych Osobowych IAS w Gdańsku (załącznik do zarządzenia nr 45/2020 Dyrektora Izby Administracji Skarbowej w Gdańsku z dnia 16 czerwca 2020 r. (w treści tej umowy w § 15 „zachowanie poufności” oraz w załączniku nr 1 do umowy – Oświadczenie Wykonawcy o Ochronie Informacji).

Każdy podmiot wykonujący dla tut. Izby Administracji Skarbowej remonty w obiektach IAS/PUCS składa:

- oświadczenie o ochronie informacji,
- klauzulę o zachowaniu poufności,

potwierdzając własnoręcznym podpisem zapoznanie się z ich treścią jak też z przestrzeganiem przedmiotowego obowiązku. Dokumenty ww. są gromadzone w aktach sprawy, przy każdym przeprowadzonych remontach. Podobnie, w usługach dotyczących brakowania i archiwizacji dokumentów. W załączeniu przesłano kserokopie przyrzeczeń o zachowaniu poufności.

[Dowód, akta kontroli, str. nr 329-1-333, 482-537]

Szkolenia z zasad ochrony danych osobowych

Każda osoba, która przetwarza dane osobowe przechodzi szkolenie z ochrony i bezpieczeństwa danych osobowych. Szkolenie odbywa się w dwóch etapach – szkolenie wstępne podczas przyjmowania do pracy oraz dalsze szkolenie na platformie e - learningowej Atena2.

W ramach szkolenia wstępnego nowo przyjęty pracownik jest zobowiązany do zapoznania się z Regulaminem użytkownika stanowiącym załącznik nr 7 do niniejszej polityki i ogólnymi zasadami przetwarzania danych osobowych na podstawie wewnętrznie przygotowanych materiałów oraz złożenia oświadczenia zgodnie z załącznikiem nr 8. Regulamin użytkownika obowiązuje wszystkie osoby przetwarzające dane osobowe w Izbie.

Szkolenia są środkiem ochrony danych osobowych od strony poufności, integralności oraz rozliczalności.

Nowoprzyjęci pracownicy przechodzą w/w szkolenia w momencie zatrudnienia.

Kontrolujący sprawdzili wywiązanie się osób świadczących pracę w US w Słupsku z obowiązku szkolenia na platformie Atena 2 oraz szkoleń na platformie MOODLE o następującej tematyce.

1. Naruszenie ochrony danych - 2201-IWD-0140.20.2022 z 31.05.2022 r.
2. Zasady bezpieczeństwa informacji - 2201-IWD-0140.1.2023 z 02.01.2023 r.

Szkolenia te są obowiązkowe na podstawie wytycznych DIAS, zawartych w w/w pismach.

Kontrolujący ustalili że na 98 zatrudnionych:

Lp.	Nazwa kursu, platforma szkoleniowa	Ilość osób, które nie odbyły kursu	% ogółu zatrudnionych w US Słupsk, którzy odbyli kurs
1.	RODO – Atena 2	28	83,03
2.	Naruszenie ochrony danych - MOODLE	24	85,45
3.	Zasady bezpieczeństwa informacji - MOODLE	17	89,70

[Dowód: akta kontroli, str. nr 65-84]

Wypełnianie obowiązku informacyjnego

Osoby, których dane dotyczą, w przypadku zbierania danych bezpośrednio od nich lub od innych osób mają prawo do informacji, o których mowa w art. 13 oraz odpowiednio w art.14 RODO. W tym zakresie każdorazowo należy uwzględnić treść art. 3 i 4 uODO.

Zgodnie z art. 47d ust 1 ustawy o KAS obowiązek o którym mowa w art. 13 RODO wobec zewnętrznych podmiotów danych realizowany jest poprzez udostępnienie klauzuli informacyjnej w Biuletynie Informacji Publicznej oraz na tablicach informacyjnych w siedzibach organów KAS, chyba że przepisy szczególne stanowią inaczej. Podczas zbierania danych osobowych, podmioty danych informowane są przez pracowników i funkcjonariuszy Izby o miejscach realizacji obowiązku informacyjnego. Obowiązek informacyjny wobec wewnętrznych podmiotów danych – pracowników i funkcjonariuszy Izby realizowany w trakcie naborów oraz w postaci klauzul informacyjnych dołączonych do dokumentów wewnętrznych np. wniosków, instrukcji, regulaminów lub publikacji na stronie intranetowej Izby. Właściciel aktywów jest odpowiedzialny za przygotowanie oraz zakomunikowanie właściwej klauzuli informacyjnej.

Kontrolujący dokonali oględzin ogólnodostępnych pomieszczeń budynku urzędu. Na drzwiach oraz tablicach informacyjnych zostały wywieszone klauzule informacyjne o których mowa wyżej.

Brak uwag.

[Dowód: akta kontroli, str. nr 324]

Ustalenia:

1. Osoba odpowiedzialna za realizację zadań z zakresu ochrony danych osobowych zobligowana jest do prowadzenia ewidencji wszystkich osób upoważnionych do przetwarzania danych osobowych (stażystów, praktykantów, pracowników firm zewnętrznych itd.). W US w Słupsku **ewidencja upoważnień prowadzona jest jedynie w stosunku do części praktykantów.**
2. **Cztery osoby spośród 25 nie otrzymały upoważnienia do przetwarzania danych osobowych**, o którym mowa w Procedurze nadawania i odwoływania upoważnień imiennych do przetwarzania danych osobowych (zał. nr 5 do Polityki Ochrony Danych Osobowych), a wszyscy pozostali **otrzymali je już po rozpoczęciu stażu/praktyki (w 1-14 dniu).**
3. Zgodnie z Polityką Ochrony Danych Osobowych, każda osoba, która przetwarza dane osobowe zobowiązana jest odbyć szkolenie z ochrony i bezpieczeństwa danych. Nie wszyscy stażysty/praktykanci zostali odpowiednio przeszkoleni - dwóch z nich **nie przeszło takiego szkolenia**, ponadto jedną osobę **przeszkolono w drugim dniu odbywania stażu**, również jedna osoba **nie złożyła podpisu na oświadczeniu** zapoznania się i przyjęcia do stosowania zasad zawartych w dokumentacji ochrony danych osobowych.
4. **Żadne z podpisanych oświadczeń o zachowaniu poufności** przez pracowników firm zewnętrznych **nie zawiera daty jego podpisania**, co uniemożliwia weryfikację okresu, od którego obowiązuje ono danego pracownika.
5. Kontrolujący stwierdzili, że do dnia wszczęcia kontroli:
 1. 48% zatrudnionych nie zapoznało się z Polityką ochrony danych Osobowych IAS w Gdańsku;
 2. 17% zatrudnionych nie odbyło obowiązkowego szkolenia RODO na platformie Atena-2;

3. 15% zatrudnionych nie odbyło obowiązkowego szkolenia „Naruszenie ochrony danych” (platforma MOODLE);
4. 10% zatrudnionych nie odbyło obowiązkowego szkolenia „Zasady bezpieczeństwa informacji” (platforma MOODLE).

Ocena częściowa:

Działalność Urzędu Skarbowego w Słupsku, w zakresie wydawania i unieważniania upoważnień, szkoleń wstępnych, prowadzenia szkoleń w zakresie ochrony danych, należy ocenić **negatywnie**.

Zagadnienie trzecie z zakresu badania:

Uprawnienia do systemów informatycznych.

Stan prawny:

Regulacje zewnętrzne

1. 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);
2. Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (t.j. Dz. U. z 2019 r. poz. 1781);
3. Ustawa z dnia 16 listopada 2016 o Krajowej Administracji Skarbowej (Dz. U. z 2022 r., poz. 813 ze zm.);
4. Ustawa z dnia 29 sierpnia 1997 r. Ordynacja podatkowa (t.j. Dz. U. z 2022 r. poz. 2651 ze zm.);

Regulacje wewnętrzne:

1. Zarządzenie Dyrektora Izby Administracji Skarbowej w Gdańsku w sprawie wprowadzenia Polityki Ochrony Danych Osobowych (45/2020 z 16 czerwca 2020 r.);
2. Zarządzenie Ministra Finansów, Funduszy i Polityki Regionalnej z dnia 29 grudnia 2020 r. w sprawie wprowadzenia Polityki Ochrony Danych Osobowych;
3. Zarządzenie nr 120/2021 Dyrektora Izby Administracji Skarbowej w Gdańsku z dnia 30 września 2021 r. w sprawie nadania regulaminu organizacyjnego Izbie Administracji Skarbowej w Gdańsku;
4. Zarządzenie nr 3/2022 Dyrektora Izby Administracji Skarbowej w Gdańsku z dnia 10 stycznia 2022 r. w sprawie nadania regulaminu organizacyjnego Izbie Administracji Skarbowej w Gdańsku;
5. Zarządzenie nr 61/2022 Dyrektora Izby Administracji Skarbowej w Gdańsku z dnia 9 maja 2022 r. w sprawie zmiany regulaminu organizacyjnego Izby Administracji Skarbowej w Gdańsku;

6. Zarządzenie nr 119/2022 Dyrektora Izby Administracji Skarbowej w Gdańsku z dnia 29 listopada 2022 r. w sprawie nadania regulaminu organizacyjnego Izbie Administracji Skarbowej w Gdańsku;
7. Upoważnienie nr 254/2021 z dnia 13.08.2021 r. do wykonywania zadań administratora danych w Urzędzie Skarbowym w Słupsku;
8. Zarządzenia Dyrektora Izby Administracji Skarbowej w Gdańsku w sprawie wprowadzenia instrukcji „Postępowanie z informacjami stanowiącymi tajemnicę skarbową w Izbie Administracji Skarbowej w Gdańsku”;
9. Decyzja nr 323/2022 Dyrektora Izby Administracji Skarbowej w Gdańsku z dnia 29 września 2022 r. w sprawie powołania Zespołu Reagowania na Incydenty Bezpieczeństwa w Izbie Administracji Skarbowej w Gdańsku;
10. Decyzja nr 143/2020 Dyrektora izby Administracji Skarbowej w Gdańsku z dnia 21 lipca 2020 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;
11. Decyzja nr 62/2022 Dyrektora izby Administracji Skarbowej w Gdańsku z dnia 2 marca 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;
12. Decyzja nr 209/2022 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;
13. Pismo Dyrektora Izby Administracji Skarbowej w Gdańsku nr 2201-IWD.0140.15.2020.1 z dnia 21.10.2020 r.;
14. Pismo Dyrektora Izby Administracji Skarbowej w Gdańsku nr 2201-IWD.0140.3.2021.1 z dnia 08.02.2021 r.;
15. Pismo Dyrektora Izby Administracji Skarbowej w Gdańsku nr 2201-IWD.0140.10.2021.1 z dnia 25.03.2021 r.;
16. Pismo Dyrektora Izby Administracji Skarbowej w Gdańsku nr 2201-IWD.0140.13.2021.2 z dnia 30.04.2021 r.;
17. Pismo Dyrektora Izby Administracji Skarbowej w Gdańsku nr 2201-IWD.0140.15.2021 z dnia 13.05.2021 r.;
18. Pismo Dyrektora Izby Administracji Skarbowej w Gdańsku nr 2201-IWD-0140.2.2022.2 z dnia 12.01.2022 r.;
19. Pismo Dyrektora Izby Administracji Skarbowej w Gdańsku nr 2201-IWD-0140.11.2022.3 z dnia 30.03.2022 r.;
20. Pismo Dyrektora Izby Administracji Skarbowej w Gdańsku nr 2201-IWD-0140.20.2022 z dnia 31.05.2022 r.;
21. Pismo Dyrektora Izby Administracji Skarbowej w Gdańsku nr 2201-IWD.0140.26.2022 z dnia 22.07.2022 r.;
22. Pismo Dyrektora Izby Administracji Skarbowej w Gdańsku nr 2201-IWD-0140.1.2023 z dnia 02.01.2023 r.;
23. Regulaminy organizacyjne Urzędu Skarbowego w Słupsku, obowiązujące w kontrolowanym okresie.

Opis stanu faktycznego:

Zgodnie z Polityką, upoważnienia i uprawnienia ewidencjonowane są w systemie informatycznym. Nie rzadziej niż raz do roku dokonywana jest analiza aktualności upoważnień i uprawnień nadanych pracownikom danego urzędu. Przeglądu dokonują kierujący komórkami pod kątem upoważnień i uprawnień wydanych pracownikom oraz ich zakresu. Ustalają również czy nie są nadane uprawnienia osobom, które zakończyły pracę.

Upoważnienia są środkiem ochrony danych osobowych od strony poufności, integralności i rozliczalności.

Jedną z zasad dotyczących uprawnień, opisanych w Polityce jest minimalizacja dostępu (Privacy by Default).

Uprawnienia w systemach informatycznych wspierających przetwarzanie czynności przetwarzania danych osobowych nadawane są w oparciu o potrzeby kierujących nimi przełożonych. Przy nadawaniu uprawnień należy kierować się zasadą minimalnych uprawnień, tj.: takich, które nie wykraczają poza potrzeby wykonania powierzonych pracownikowi zadań. Należy kierować się także zasadą mówiącą, że jeśli coś nie jest wyraźnie dozwolone to jest zakazane.

Stosowanie zasady Privacy By Default jest środkiem ochrony danych osobowych od strony poufności. Do 21.06.2022 r. sprawę zarządzania uprawnieniami regulowała Instrukcja I-096/1 „Zarządzanie uprawnieniami do systemów informatycznych w Izbie Administracji Skarbowej w Gdańsku, Urzędach Skarbowych woj. pomorskiego oraz w Pomorskim Urzędzie Celno – Skarbowym w Gdyni” stanowiąca załącznik do Zarządzenia nr 73/2018 Dyrektora IAS w Gdańsku z 4 grudnia 2018 r.

Obecnie te sprawy reguluje Instrukcja I-112/1, o tym samym tytule, stanowiąca załącznik do Zarządzenia nr 30/2023 (obowiązuje od 31.03.2023 r.)

Zgodnie z § 10 ust. 1 I- 096/1, bezpośredni przełożony dokonuje przeglądu praw dostępu do zasobów teleinformatycznych posiadanych przez podległych pracowników co najmniej dwa razy w roku do 30 czerwca i do 31 grudnia danego roku oraz każdorazowo w przypadku zmian organizacyjnych oraz zmian w zakresach obowiązków pracowników.

Kontrolujący sprawdzili, czy kierujący komórkami organizacyjnymi dokonują okresowego (raz do roku) przeglądu nadanych uprawnień. Wszyscy kierownicy oświadczyli, że dokonywali przeglądu uprawnień nadanych podległym pracownikom zgodnie z §10 Instrukcji I-096/1.

[Dowód, akta kontroli, str. nr 408-424]

Kontrolujący sprawdzili terminowość i zasadność nadawania i odbierania uprawnień do wybranych systemów teleinformatycznych oraz blokowania kont domenowych, dla wybranych pracowników US w Słupsku. Są to osoby, które przebywają lub wróciły z długoterminowych nieobecności. W tym celu poprosili Kierownika Działu IWO oraz CIRF o odpowiednie zestawienia z systemu w którym zaewidencjonowane są takie zdarzenia. Poniżej zestawienie na podstawie otrzymanych danych:

Lp.	Pracownik	Data nieobecności	Czy zablokowano dostęp do domeny (tak/nie)	Czy odebrano uprawnienia do systemów	Uwagi

Lp.	Pracownik	Data nieobecności	Czy zablokowano dostęp do domeny (tak/nie)	Czy odebrano uprawnienia do systemów	Uwagi
1.	M.A.	01.01.2022 – 28.02.2023	TAK	-	BRAK ODNOTOWANYCH UPRAWNIENI W SYSUP
2.	A.B.	01.01.2022 – 21.10.2022	TAK	TAK	Widoczne uprawnienia nadano po 21.10.2022; w trakcie nieobecności nadano je do jednego systemu: BPS.
3.	A.C.	23.01.2022 – 30.06.2022	TAK	NIE	-
4.	K.K.	07.02.2022 – 05.02.2023	TAK	NIE	-
5.	M.K.	01.01.2022 – 09.09.2022	TAK	TAK	Widoczne uprawnienia nadano po 09.09.2022; nie odebrano uprawnień do CEKR/CEKR2 i SZD.
6.	A.K.	31.01.2022 – 03.01.2023	TAK	NIE	Wnioski o wycofanie złożono w dniu 10.05.2023 r.
7.	M.D.	01.01.2022 – 11.04.2022 16.05.2022 – 30.09.2022	TAK	TAK/NIE	Konto domenowe wyłączone w dniu 01.06.2021 r.; Do części systemów nadano uprawnienia po 30.09.2022 r., do pozostałej części nie odebrano ich.
9.	M.O.	01.01.2022 – 28.02.2023	TAK	TAK	-
10.	K.P.	03.10.2022 – 16.02.2023	TAK	NIE DOTYCZY	-
11.	L.P.	31.01.2022 – 28.02.2023	TAK	NIE	Konto domenowe wyłączone w dniu 25.04.2023 r.; 31.01.2023 r. odebrano uprawnienia do SeRCe KEP
12.	K.S.	02.02.2022 – 31.01.2023	TAK	NIE	-

Lp.	Pracownik	Data nieobecności	Czy zablokowano dostęp do domeny (tak/nie)	Czy odebrano uprawnienia do systemów	Uwagi
13.	A.Ś.	17.08.2022 – 14.02.2023	NIE	NIE DOTYCZY	-
14.	I.P.	18.10.2022 – 28.02.2023	TAK	NIE DOTYCZY	Konto domenowe wyłączzone w dniu 12.04.2023 r.
15.	A.Z.	01.01.2022 – 20.05.2022	TAK	NIE	-
16.	A.Z2	02.05.2022 – 05.09.2022	NIE	NIE	-
17.	M.Z.	08.08.2022 – 22.12.2022	TAK	NIE DOTYCZY	Konto domenowe wyłączzone w dniu 12.04.2023 r.
18.	M.Z2	01.01.2022 – 28.02.2023	TAK	-	BRAK ODNOTOWANYCH UPRAWNIEN W SYSUP

[Dowód: akta kontroli, str. nr 557 - 620]

Zbadano również nadzór Naczelnika nad dostępem i wykorzystywaniem tzw. aplikacji zewnętrznych. Zgodnie z § 8 obowiązującej do 21.06.2022 r. I-096/1, w ramach zarządzania procesem dostępu do zewnętrznych zasobów informatycznych, zlokalizowanych poza siedzibą Izby oraz poza siedzibami urzędów, posiadających własne polityki bezpieczeństwa, stosuje się zasady opisane w dokumentacji tych aplikacji lub zalecenia przekazane przez administratora systemu.

W celu uzyskania dostępu do aplikacji zewnętrznej:

- Bezpośredni przełożony pracownika sporządza wniosek według właściwego wzoru dla danej aplikacji, przy uwzględnieniu ewentualnych limitów dostępowych do danej aplikacji w uzgodnieniu z administratorem merytorycznym aplikacji. Zatwierdzony zgodnie z procedurą akceptacji wniosek bezpośredni przełożony pracownika przekazuje do realizacji zgodnie z obowiązującymi procedurami zarządzania użytkownikami dla danej aplikacji.
- **Skan zatwierdzonego wniosku przekazywany jest do administratora aplikacji SysUp odpowiedzialnego za rejestr uprawnień użytkowników aplikacji zewnętrznych, który wprowadza do aplikacji informację o uprawnieniach dla danego pracownika;**
- Po otrzymaniu informacji zwrotnej o realizacji wniosku użytkownik aplikacji zewnętrznej lub jego bezpośredni przełożony zobowiązany jest do poinformowania drogą e-mail ASI, przekazując kopię informacji zwrotnej (mail, skan potwierdzenia realizacji wniosku, skan nadanych uprawnień, itp.);
- Administrator merytoryczny odpowiedzialny za rejestr uprawnień w aplikacjach zewnętrznych odnotowuje w SysUp informacje o założonym lub zamkniętym koncie oraz o nadanych lub odebranych uprawnieniach danego pracownika.

Kontrolujący wystąpili do Naczelnika z wnioskiem o przekazanie listy osób z urzędu, którzy mają dostęp do następujących aplikacji:

- 1) CEPiK (Centralna Ewidencja Pojazdów i Kierowców),
- 2) eKW (elektroniczne księgi wieczyste),
- 3) Rejestr Zastawów Skarbowych,
- 4) Rejestr Należności Publicznoprawnych

oraz zapytali, czy uprawnienia dostępu do w/w aplikacji zewnętrznych były w jakikolwiek sposób ewidencjonowane przez kierowników komórek organizacyjnych, a także w jakich systemach.

Odpowiedź:

Dostęp do systemu CEPiK wskazani pracownicy wykorzystują wyłącznie do celów służbowych, tj. realizacji zadań komórki organizacyjnej Działu Egzekucji Administracyjnej oraz Trzeciego Referatu Czynności Analitycznych i Sprawdzających m.in. w sprawie zadań w obszarze NZP/nieujawnionych źródeł przychodów oraz w obszarze informacji sygnałnych. W przypadku konieczności uzyskania stosownych danych, pracownik podaje sygnaturę (nr) sprawy, w związku z którą pozyskuje informacje oraz do której zostaną załączone pozyskane dane.

Dostęp do CEPiK są niezbędne z uwagi na wykonywane przez pracowników Referatu Podatku Akcyzowego i Podatku od Gier działania w zakresie opodatkowania samochodów. Taki dostęp powinni mieć wszyscy pracownicy Referatu jednakże z uwagi na ograniczoną ich ilość dostęp ma kierownik i trzech pracowników. Kierownik SPA prowadzi własną ewidencję dostępu do aplikacji CEPiK - przechowuje w wydzielonym folderze elektroniczne kopie wniosków o nadanie/cofnięcie uprawnień do systemu.

Ponadto Naczelnik wskazał, że kierownicy pracowników posiadających uprawnienia do systemów: CEPiK, eKW, Rejestru Zastawów Skarbowych oraz Rejestru Należności Publicznoprawnych prowadzą własne ewidencje certyfikatów, ponieważ ww. systemy posiadają własne polityki bezpieczeństwa oraz własne wnioski o nadanie uprawnień.

[Dowód, akta kontroli, str. nr 398-402, 633 - 636]

Ponadto zapytaliśmy Naczelnika w jaki sposób w urzędzie sprawowany był nadzór nad właściwym wykorzystaniem w/w aplikacji oraz czy zwracał się do właścicieli biznesowych tych aplikacji o dane dotyczące ilości i dat logowań do systemu osób uprawnionych oraz przypadków wprowadzania niewłaściwego ciągu znaków lub nieadekwatnych danych w polu służącym do weryfikacji zasadności dostępu do informacji.

Używanie przez pracowników w/w, przykładowych aplikacji do celów innych niż służbowe łamie podstawowe zasady bezpieczeństwa informacji:

- zasadę przywilejów koniecznych – oznaczającej, że każdy pracownik posiada prawo dostępu do informacji ograniczone wyłącznie do tych, które są konieczne do realizacji powierzonych zadań,
- zasadę wiedzy koniecznej – oznaczającej, że każdy pracownik posiada wiedzę o zasobie, do którego ma dostęp, ograniczoną wyłącznie do zagadnień, które są konieczne do realizacji powierzonych zadań.

Przegląd w/w uprawnień jest środkiem ochrony danych osobowych od strony poufności, integralności i rozliczalności.

Naczelnik wskazał że pracownicy wielokrotnie przeszli szkolenia z zakresu ochrony danych osobowych i są świadomi, że informacje zawarte w systemie nie mogą być wykorzystywane do innych celów niż związanych z wykonywanymi zadaniami. W systemie obowiązani są podać numer sprawy lub pisma z powodu którego pozyskiwali dane. System posiada możliwość wydruku do 200 ostatnich zapytań poczynionych przez pracownika (CEPiK). Natomiast Naczelnik nie udzielił odpowiedzi na pytanie, czy zwracał się do właścicieli biznesowych tych aplikacji o dane dotyczące ilości i dat logowań do systemu osób uprawnionych oraz przypadków wprowadzania niewłaściwego ciągu znaków lub nieadekwatnych danych w polu służącym do weryfikacji zasadności dostępu do informacji.

[Dowód: akta kontroli, str. nr 398-402]

Kontrolujący wystąpili również do Ministerstwa Finansów, Departamentu Poboru Podatków, jako właściciela biznesowego kluczowych aplikacji używanych w urzędach skarbowych, z wnioskiem o udostępnienie logowań do domeny, w czasie nieobecności pracownika wskazanego pracownika. Tabela poniżej:

Lp.	Imię, nazwisko	Login AD	Okres
1.	M.B.	(...)	12.09.2022 – 20.09.2022
2.	A.B.	(...)	18.08.2022 – 02.09.2022
3.	B.C.	(...)	22.09.2022 – 06.10.2022
4.	P.G.	(...)	16.08.2022 – 29.08.2022
5.	E.K.	(...)	27.01.2023 – 10.02.2023
6.	A.L.	(...)	23.08.2022 – 02.09.2022
7.	L.Ł.	(...)	18.08.2022 – 26.08.2022
8.	A.M.	(...)	10.08.2022 – 01.09.2022
9.	A.M2	(...)	29.07.2022 – 16.08.2022
10.	T.N.	(...)	30.05.2022 – 24.06.2022
11.	A.W.	(...)	11.04.2022 – 15.04.2022
12.	A.P.	(...)	17.10.2022 – 26.10.2022
13.	A.S.	(...)	22.08.2022 – 24.08.2022
14.	W.S.	(...)	29.12.2022 – 18.01.2023
15.	I.U.	(...)	14.07.2022 – 01.08.2022
16.	M.A.	(...)	01.01.2022 – 28.02.2023
17.	A.B2	(...)	01.01.2022 – 21.10.2022
18.	A.C.	(...)	23.01.2022 – 30.06.2022

Lp.	Imię, nazwisko	Login AD	Okres
19.	K.K.	(...)	07.02.2022 – 05.02.2023
20.	M.K.	(...)	01.01.2022 – 09.09.2022
21.	A.K.	(...)	31.01.2022 – 03.01.2023
22.	M.D.	(...)	01.01.2022 – 11.04.2022 16.05.2022 – 30.09.2022
23.	M.M.	(...)	02.11.2022 – 03.01.2023 25.01.2023 – 28.02.2023
24.	M.O.	(...)	01.01.2022 – 28.02.2023
25.	K.P.	(...)	03.10.2022 – 16.02.2023
26.	L.P.	(...)	31.01.2022 – 28.02.2023
27.	K.S.	(...)	02.02.2022 – 31.01.2023
28.	A.Ś.	(...)	17.08.2022 – 14.02.2023
29.	I.P.	(...)	18.10.2022 – 28.02.2023
30.	A.Z.	(...)	01.01.2022 – 20.05.2022
31.	A.Z2	(...)	02.05.2022 – 05.09.2022
32.	M.Z.	(...)	08.08.2022 – 22.12.2022
33.	M.Z2	(...)	01.01.2022 – 28.02.2023
34.	J.Z.	(...)	26.02.2022 – 31.05.2022

Odpowiedź Departamentu Poboru Podatków Ministerstwa Finansów brzmi:

W okresach wskazanych w naszym piśmie z 26 kwietnia 2023 roku **nie odnotowano logowań, loginów / zapytań pochodzących od wymienionych osób** do następujących systemów / aplikacji, których jest Właścicielem Biznesowym:

- Scentralizowany System Poboru (SSP),
- Poltax2BPlus,
- Serwis Ksiąg Wieczystych Ministerstwa Sprawiedliwości dla Ministerstwa Finansów,
- Rejestr Należności Publicznoprawnych (RNP).

W okresach wskazanych **nie odnotowano** także logowań 7 użytkowników do Systemu Rejestracji Centralnej (SeRCe).

Dodatkowo ustalono, że pozostałe osoby (które wskazano w załączonym zestawieniu) nie posiadają uprawnień do systemu SeRCe, jako pracownicy Urzędu Skarbowego w Słupsku.

W odniesieniu do systemu PoltaxPlus, Departament DPP informuje, że nie ma możliwości pozyskania wnioskowanych informacji - w logach PoltaxPlus, brak jest informacji o logowaniu do systemu.

Podobnie, w przypadku Rejestru Zastawów Skarbowych oraz w systemie EGAPOLTAX, nie jest technicznie możliwe sprawdzenie przedmiotowych logowań we wskazanych okresach.

Także w obecnej konstrukcji Hurtowni Danych SPR nie przewidziano zachowywania danych logowań użytkowników.

W odniesieniu do aplikacji REMDAT – brak dostępu wymienionych osób do aplikacji.

Zintegrowany System Poboru Należności i Rozrachunków z UE i Budżetem (Zefir2) – odnotowano logowanie 1 użytkownika – Pani M.D.. Tego logowania dokonano z komputera nr (...), który użytkował wtedy Pan M.M..

Poprosiliśmy Naczelnika o wyjaśnienie tej sprawy. Pani M.D. oraz pan M.M. złożyli wyjaśnienia w których zgodnie stwierdzili, że nigdy nie przekazywali danych służących do logowań domeny MF (login, hasło). Ponadto Pani M.D. stwierdziła, że nigdy nie uzyskała dostępu systemu ZEFIR2. Potwierdziła to jej bezpośrednia przełożona – Pani A.B..

Zwróciliśmy się z prośbą do Departamentu Poboru Podatków MF o ponowne zbadanie tej sprawy. Otrzymaliśmy odpowiedź, że po pogłębionej weryfikacji aktywności w logach systemu Zefir2 dla wymienionych wyżej użytkowników, we wskazanym okresie, **nie odnotowano aktywności / logowań**.

[Dowód: akta kontroli, str. nr 538 – 540, 551, 556, 622, 632, 651 - 654]

Zgodnie z § 7 ust. 5 I-096/1 (obowiązującej do 21.06.2022), przypadku długotrwałej nieobecności pracownika (dłuższej niż 3 miesiące) bezpośredni przełożony wnioskuje o zablokowanie konta domenowego. Kontrolujący poprosili kierowników jednostek organizacyjnych US w Słupsku o złożenie oświadczeń, czy wnioskowali o zablokowanie kont domenowych podległych pracowników, o których wiedzieli, że ich nieobecność trwa już 3 miesiące.

Niżej wymienieni kierownicy złożyli oświadczenia:

Lp.	Imię, Nazwisko kierownika	Komórka organizacyjna	Podległy pracownik (Imię, nazwisko)	Czy wystąpiono o zablokowanie konta domenowego (tak/nie)	Uwagi
1.	A.M.	Referat SKI	M.Z. A.B.	TAK	-
2.	A.W.	Referat SWW	A.Z.	NIE	Na dzień uchylecia obowiązywania Instrukcji I-096/1 nieobecność pracownika nie przekraczała 3 m-cy
3.	W.S.	Referat SKA-3	K.S. I.P. M.Z2	TAK	-
4.	A.P.	Dział SER	A.K.	TAK	-

Lp.	Imię, Nazwisko kierownika	Komórka organizacyjna	Podległy pracownik (Imię, nazwisko)	Czy wystąpiono o zablokowanie konta domenowego (tak/nie)	Uwagi
5.	K.Z.	Dział SOB-1	K.K. M.O.	NIE	M.O. – konto zablokowane 10.05.2023 r.
6.	A.S.	Dział SKV	L.P.	NIE	Konto zablokowane 24.04.2023 r.
7.	I.U.	Dział SEW	J.Z.	NIE	Brak zasadności – pracownik wrócił do pracy po 3 mies i 5 dniach
8.	B.C.	Dział SOB-2	M.A. A.Z2	NIE	M.A. – nieobecna od 4 lat, konto zablokowane
9.	A.B2	Dział SKA-2	A.C. M.K. M.D.	NIE	-

Naczelnik oraz kierownicy wskazali, że wnioski o zablokowanie kont domenowych składali przez CSD lub e-mail do pracownika CIRF.

[Dowód: akta kontroli, str. nr 633 – 634, 637 - 648]

Zgodnie z § 4 ust 6, pkt 1 lit. d, pkt 2 I-096/1 Pracownicy Wydziału Kadr Izby na bieżąco przekazują informacje na temat długotrwałej (powyżej 3 miesięcy) nieobecności pracownika.

Informacja ta powinna zawierać imię i nazwisko pracownika, praktykanta, stażysty oraz innej osoby świadczącej pracę na rzecz Izby, nazwę komórki organizacyjnej, określenie miejsca świadczenia pracy lub służby oraz początkową datę długotrwałej nieobecności lub/oraz datę powrotu do pracy lub służby. Informacje należy przekazywać drogą elektroniczną jako wiadomość e-mail do: IOD (...) oraz do ówczesnego Wydziału Informatyki Izby (...).

Poprosiliśmy I Zastępcę Dyrektora IAS o informację, czy podlegli mu pracownicy dopełnili tego obowiązku w stosunku do osób długotrwale nieobecnych (powyżej 3 miesięcy).

Odpowiedź Naczelnika Pierwszego Działu Kadr i Administracji Personalnej IAS w Gdańsku brzmi, że na 16 przypadków długotrwałych nieobecności tylko 2 razy poinformowano odpowiednie służby o tym fakcie.

[Dowód: akta kontroli, str. nr 649 – 650]

Ustalenia:

Załącznik nr 21 do instrukcji I-086

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

1. Uprawnienia do aplikacji zewnętrznych (Elektroniczne Księgi Wieczyste, Rejestr Zastawów Skarbowych, Rejestr Należności Publicznoprawnych, CEPiK) **nie zostały zarejestrowane w obowiązującym Systemie Rejestrowania Uprawnień (SysUp), na Portalu Pracownika.** Kierownicy komórek organizacyjnych, wbrew zapisom § 8 Instrukcji I-096/1 „Zarządzanie uprawnieniami do systemów informatycznych w Izbie Administracji Skarbowej w Gdańsku, Urzędach Skarbowych woj. pomorskiego oraz w Pomorskim Urzędzie Celno – Skarbowym w Gdyni”, stanowiącej załącznik do Zarządzenia nr 73/2018 Dyrektora IAS w Gdańsku z 4 grudnia 2018 r., obowiązującej do 21.06.2022 r., nie przekazali zatwierdzonych wniosków o uprawnienia do w/w aplikacji do administratora aplikacji SysUp, odpowiedzialnego za rejestr uprawnień użytkowników aplikacji zewnętrznych, który wprowadza do aplikacji informację o uprawnieniach dla danego pracownika. Ewidencja osób upoważnionych do pracy w tych systemach jest prowadzona tylko w wewnętrznie, w nich samych. Niezaewidencjonowanie uprawnień do zewnętrznych systemów informatycznych, w jednolitym rejestrze (wtedy – SysUp), pozbawia Naczelnika oraz poszczególnych kierowników skutecznego narzędzia do sprawowania nadzoru nad nimi.
2. Naczelnik **nie sprawował skutecznego nadzoru nad właściwym wykorzystaniem w/w aplikacji zewnętrznych.** Nie zwrócił się w kontrolowanym okresie do właścicieli biznesowych tych aplikacji o dane dotyczące ilości i dat logowań do systemu osób uprawnionych oraz przypadków wprowadzania niewłaściwego ciągu znaków lub nieadekwatnych danych w polu służącym do weryfikacji zasadności dostępu do informacji. Ewentualne używanie przez pracowników w/w, przykładowych aplikacji do celów innych niż służbowe łamie podstawowe zasady bezpieczeństwa informacji:
 - zasadę przywilejów koniecznych – oznaczającej, że każdy pracownik posiada prawo dostępu do informacji ograniczone wyłącznie do tych, które są konieczne do realizacji powierzonych zadań,
 - zasadę wiedzy koniecznej – oznaczającej, że każdy pracownik posiada wiedzę o zasobie, do którego ma dostęp, ograniczoną wyłącznie do zagadnień, które są konieczne do realizacji powierzonych zadań.
3. Część kierowników nie wnioskowała o odebranie dostępu do domeny MF dla długotrwale nieobecnych pracowników (dłuższej niż 3 miesiące). Złamali tym samym zapisy § 7 ust. 5 I-096/1 (obowiązującej do 21.06.2022). Blokowanie dostępu do domeny jest w tym przypadku kluczowe. Takie postępowanie wyklucza możliwość dostępu do ogromnej większości używanych w urzędzie aplikacji.

Ocena częściowa:

Działalność Urzędu Skarbowego w Słupsku, w zakresie uprawnień do systemów informatycznych, należy ocenić **negatywnie**.

Zagadnienie czwarte z zakresu badania:

Ochrona informacji - tajemnicy skarbowej.

Stan prawny:

Regulacje zewnętrzne:

1. Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (t.j. Dz. U. z 2019 r. poz. 1781);

2. Ustawa z dnia 16 listopada 2016 o Krajowej Administracji Skarbowej (Dz. U. z 2022 r., poz. 813 ze zm.);
3. Ustawa z dnia 29 sierpnia 1997 r. Ordynacja podatkowa (t.j. Dz. U. z 2022 r. poz. 2651 ze zm.);

Regulacje wewnętrzne:

1. Zarządzenie nr 120/2021 Dyrektora Izby Administracji Skarbowej w Gdańsku z dnia 30 września 2021 r. w sprawie nadania regulaminu organizacyjnego Izbie Administracji Skarbowej w Gdańsku;
2. Zarządzenie nr 3/2022 Dyrektora Izby Administracji Skarbowej w Gdańsku z dnia 10 stycznia 2022 r. w sprawie nadania regulaminu organizacyjnego Izbie Administracji Skarbowej w Gdańsku;
3. Zarządzenie nr 61/2022 Dyrektora Izby Administracji Skarbowej w Gdańsku z dnia 9 maja 2022 r. w sprawie zmiany regulaminu organizacyjnego Izby Administracji Skarbowej w Gdańsku;
4. Zarządzenie nr 119/2022 Dyrektora Izby Administracji Skarbowej w Gdańsku z dnia 29 listopada 2022 r. w sprawie nadania regulaminu organizacyjnego Izbie Administracji Skarbowej w Gdańsku;
5. Upoważnienie nr 254/2021 z dnia 13.08.2021 r. do wykonywania zadań administratora danych w Urzędzie Skarbowym w Słupsku;
6. Zarządzenia Dyrektora Izby Administracji Skarbowej w Gdańsku w sprawie wprowadzenia instrukcji „Postępowanie z informacjami stanowiącymi tajemnicę skarbową w Izbie Administracji Skarbowej w Gdańsku”;
7. Decyzja nr 323/2022 Dyrektora Izby Administracji Skarbowej w Gdańsku z dnia 29 września 2022 r. w sprawie powołania Zespołu Reagowania na Incydenty Bezpieczeństwa w Izbie Administracji Skarbowej w Gdańsku;
8. Decyzja nr 143/2020 Dyrektora Izby Administracji Skarbowej w Gdańsku z dnia 21 lipca 2020 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;
9. Decyzja nr 62/2022 Dyrektora Izby Administracji Skarbowej w Gdańsku z dnia 2 marca 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;
10. Decyzja nr 209/2022 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;
11. Pismo Dyrektora Izby Administracji Skarbowej w Gdańsku nr 2201-IWD.0140.15.2020.1 z dnia 21.10.2020 r.;
12. Pismo Dyrektora Izby Administracji Skarbowej w Gdańsku nr 2201-IWD.0140.3.2021.1 z dnia 08.02.2021 r.;
13. Pismo Dyrektora Izby Administracji Skarbowej w Gdańsku nr 2201-IWD.0140.10.2021.1 z dnia 25.03.2021 r.;

14. Pismo Dyrektora Izby Administracji Skarbowej w Gdańsku nr 2201-IWD.0140.13.2021.2 z dnia 30.04.2021 r.;
15. Pismo Dyrektora Izby Administracji Skarbowej w Gdańsku nr 2201-IWD.0140.15.2021 z dnia 13.05.2021 r.;
16. Pismo Dyrektora Izby Administracji Skarbowej w Gdańsku nr 2201-IWD-0140.2.2022.2 z dnia 12.01.2022 r.;
17. Pismo Dyrektora Izby Administracji Skarbowej w Gdańsku nr 2201-IWD-0140.11.2022.3 z dnia 30.03.2022 r.;
18. Pismo Dyrektora Izby Administracji Skarbowej w Gdańsku nr 2201-IWD-0140.20.2022 z dnia 31.05.2022 r.;
19. Pismo Dyrektora Izby Administracji Skarbowej w Gdańsku nr 2201-IWD.0140.26.2022 z dnia 22.07.2022 r.;
20. Pismo Dyrektora Izby Administracji Skarbowej w Gdańsku nr 2201-IWD-0140.1.2023 z dnia 02.01.2023 r.;
21. Regulaminy organizacyjne Urzędu Skarbowego w Słupsku, obowiązujące w kontrolowanym okresie.

Opis stanu faktycznego:

Regulacje dotyczące tajemnicy skarbowej zawarte są w Dziale VII Ordynacji podatkowej. Szczegółowo to zagadnienie reguluje Zarządzenia Dyrektora Izby Administracji Skarbowej w Gdańsku w sprawie wprowadzenia instrukcji „Postępowanie z informacjami stanowiącymi tajemnicę skarbową w Izbie Administracji Skarbowej w Gdańsku” (I-037/1).

Grupa pierwsza dokumentów, to te zawierające informacje, o których mowa w treści art. 182 Ordynacji podatkowej.

Grupa druga - dokumenty nie zawierające informacji w art. 182 OP. Oznacza się je klauzulą „Tajemnica skarbową” (zgodnie z art. 299 a ustawy OP) umieszczając klauzulę na pierwszej stronie w prawym górnym rogu a ich przekazywanie następuje w trybie przewidzianym dla dokumentów jawnych. Podobnie postępuje się z przekazywaniem informacji o numerach rachunków bankowych posiadanych przez podatników, które mogą być udostępniane podmiotom określonym w tym artykule.

Grupa trzecia – wszystkie pozostałe materiały spełniające kryteria określone w art. 293 OP, które nie podlegają oznaczeniu klauzulą „Tajemnica skarbową”. Są to głównie materiały przechowywane w Izbie, ale także udostępniane między innymi ministrowi właściwemu do spraw finansów publicznych, Szefowi Krajowej Administracji Skarbowej lub innym organom podatkowym (zgodnie z art. 298 ustawy OP).

Wg oświadczenia Naczelnika, osobą odpowiedzialną za nadzór nad sprawami związanymi Tajemnicą skarbową jest Pan C.M. i Pani K.N. (oboje z SWW). W kontrolowanym okresie Naczelnik wysłał dwa dokumenty z grupy I, skierowane do Prokuratury Okręgowej w (...):

- 2216-SPV-1.493.4.2023.2
- 2216-SPV-1.4103.43.2020.40

Dokumenty stanowiące „Tajemnicę skarbową” przechowywane są w pomieszczeniu kancelarii materiałów zastrzeżonych w plombowanej i zamykanej na klucz szafie metalowej.

Brak uwag.

[Dowód: akta kontroli, str. nr 307 – 310, 398 – 407, 633 - 634]

Kontrolujący sprawdzili prowadzone zapisy w dzienniku ewidencyjnym (DE), w którym rejestrowane jest korespondencja wychodząca i przychodząca z grupy I i II dokumentów. Sprawdziliśmy wszystkie pozycje (3 w 2022 r. oraz 2 w 2023).

Brak uwag

[Dowód: akta kontroli, str. nr 307 - 310]

Sprawdziliśmy ponadto stan zapoznania się pracowników z instrukcją I-037/1. Z Instrukcją zapoznali się 144 osoby, **w tym 90 po wszczęciu kontroli. Nie zapoznało się 12 pracowników (7,7%)**

[Dowód: akta kontroli, str. nr 88 - 138]

Ustalenia:

Postępowanie w dokumentami objętymi Tajemnicą skarbową reguluje w IAS w Gdańsku Zarządzenie Dyrektora Izby Administracji Skarbowej w Gdańsku w sprawie wprowadzenia instrukcji „Postępowanie z informacjami stanowiącymi tajemnicę skarbową w Izbie Administracji Skarbowej w Gdańsku” (I-037/1). Jest ono dostępne w aplikacji Q-asystent. Pracownik potwierdza zapoznanie się z dokumentem poprzez kliknięcie ikonki „Zapoznałem się z dokumentem”. Jedną z funkcjonalności tej aplikacji jest możliwość weryfikacji zapoznania się z konkretnym dokumentem. Na tej podstawie stwierdziliśmy, że z Instrukcją tą nie zapoznało się 12 pracowników (7,7%). Zwraca uwagę fakt, że 57% pracowników zapoznało się z dokumentem po wszczęciu kontroli.

Ocena częściowa:

Działalność Urzędu Skarbowego w Słupsku, w zakresie ochrony informacji – tajemnicy skarbowej, należy ocenić **pozytywnie z uchybieniami**.

IV. Pozostałe informacje

W kontrolowanym okresie nie przeprowadzono kontroli funkcjonalnych w zakresie przestrzegania przepisów o ochronie danych osobowych oraz tajemnicy skarbowej.

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

1. Zapewnić poufność dokumentów oraz zawartych w nich informacji, a więc nie dopuszczać, aby z informacjami mogły zapoznać się osoby nieupoważnione. Dane osobowe oraz inne informacje powinny być przechowywane w zamykanych szafach, co zapewnia zabezpieczenie danych osobowych od strony poufności i integralności.
2. Przestrzegać zasady „czystego biurka”, czyli zadbać o niepozostawianie dokumentów i innych nośników informacji na stanowisku pracy (biurku) podczas nieobecności. Zapewnienie tej zasady pozwoli na to, że dane osobowe nie będą dostępne osobom nieuprawnionym do ich przetwarzania.
3. Wszystkim osobom (stażyści, praktykanci etc.), które przetwarzają dane osobowe, obligatoryjnie nadawać upoważnienia do przetwarzania danych osobowych przed rozpoczęciem przez te osoby przetwarzania w/w danych.

4. Uzupelnic brakujace oraz rejestrowac kolejne upowaznienia w ewidencji osob upowaznionych do przetwarzania danych osobowych, zgodnie z Procedura nadawania i odwoływania upowaznień imiennych do przetwarzania danych osobowych (załącznik nr 5 do Polityki Ochrony Danych Osobowych).
5. Przeprowadzac szkolenia z ochrony i bezpieczenstwa ochrony danych osobowych w stosunku do wszystkich osob (stażystow, praktykantow etc.), ktore przetwarzaja dane osobowe, przed rozpoczeciem przez te osoby przetwarzania w/w danych, a takze dokumentowac ukończenie takiego szkolenia podpisem osoby przeszkolonej.
6. Na wszystkich oświadczeniach o zachowaniu poufności oraz o zapoznaniu się i przyjęciu do stosowania zasad zawartych w dokumentacji ochrony danych osobowych, zamieszczać datę ich podpisania.
7. Zobligowac podleglych pracownikow do bezwzględnego zapoznawania się z dokumentacją zamieszczaną w aplikacji Q-asystent (oraz potwierdzania tego faktu w aplikacji).
8. Egzekwować obowiazkowe szkolenia z ochrony danych (RODO).
9. Rejestrowac w aplikacji Q-asystent wszystkie uprawnienia do systemow informatycznych (w tym te, ktorych właścicielami biznesowymi są podmioty spoza Krajowej Administracji Skarbowej).
10. Monitorowac właściwe wykorzystanie aplikacji (w tym zewnetrznych), przez sprawdzenie ilosci i dat logowañ do systemu osob uprawnionych oraz przypadków wprowadzania niewłaściwego ciągu znakow lub nieadekwatnych danych w polu służącym do weryfikacji zasadności dostępu do informacji.
11. Zaplanowac i przeprowadzić kontrole funkcjonalne w powyższym zakresie.

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 30 dni od daty otrzymania niniejszego wystąpienia pokontrolnego informacji o sposobie wykorzystania zaleceń, wykorzystania wnioskow 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 Finansow zobowiązuje do przekazania do kierownika komórki ds. kontroli tut. Izby Administracji Skarbowej informacji o rezultatach wdrożonych zaleceń pokontrolnych w terminie 9 miesiocy 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, 6 czerwca 2023 r.

Zastępcą Dyrektora
Izby Administracji Skarbowej w Gdańsku
Wioleta Gawlińska
(kwalifikowany podpis elektroniczny)