Załącznik nr 21
do instrukcji I-086/3

Krajowa Administracja Skarbowa

Izba Administracji Skarbowej w Gdańsku

2201-IWA.0921.4.2023

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 Sopocie
ul. 23 Marca 9/11
81-808 Sopot

Kierownik jednostki kontrolowanej:
Pani Joanna Trusiewicz – Naczelnik US w Sopocie.

Kontrolerzy:

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

działający na podstawie upoważnienia Dyrektora Izby Administracji Skarbowej nr 2201-IWA.0921.4.2023 z 17.03.2023 r.

Data rozpoczęcia i zakończenia czynności kontrolnych

- rozpoczęcie czynności kontrolnych - 17.03.2023 r.
- zakończenie czynności kontrolnych – 28.04.2023 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 Sopocie w badanym zakresie oceniono **pozytywnie z uchybieniami**.

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, monitoringu wizyjnego (oznaczenie obszaru, klauzula informacja, przechowywanie, udostępnianie oraz usuwanie danych z monitoringu wizyjnego). Dostępność 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 cząstkowe dotyczące kontrolowanych zagadnień.

III. Opis ustalonego stanu faktycznego

Zagadnienie pierwsze z zakresu badania:
Przestrzeganie zasad bezpieczeństwa informacji.

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 32/2018 Dyrektora Izby Administracji Skarbowej w Gdańsku z dnia 24 maja 2018 r. w sprawie wprowadzenia Regulaminu Funkcjonowania Monitoringu Wizyjnego w Izbie Administracji Skarbowej w Gdańsku.
7. 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;
8. Upoważnienie nr 79/2023 z dnia 22.02.2023 r. do wykonywania zadań administratora danych w Urzędzie Skarbowym w Sopocie;
9. Upoważnienie nr 281/2022 z dnia 06.07.2022 r. do wykonywania zadań administratora danych w Urzędzie Skarbowym w Sopocie;
10. Upoważnienie nr 232/2021 z dnia 04.08.2021 r. do wykonywania zadań administratora danych w Urzędzie Skarbowym w Sopocie;
11. Zarządzenia Dyrektora Izby Administracji Skarbowej w Gdańsku w sprawie wprowadzenia instrukcji „Postępowanie z informacjami stanowiącymi tajemnicę skarbową w Izbie Administracji Skarbowej w Gdańsku”;
12. 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;
13. 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;
14. 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;
15. 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;
16. Pismo Dyrektora Izby Administracji Skarbowej w Gdańsku nr 2201-IWD.0140.15.2020.1 z dnia 21.10.2020 r.;
17. Pismo Dyrektora Izby Administracji Skarbowej w Gdańsku nr 2201-IWD.0140.3.2021.1 z dnia 08.02.2021 r.;
18. Pismo Dyrektora Izby Administracji Skarbowej w Gdańsku nr 2201-IWD.0140.10.2021.1 z dnia 25.03.2021 r.;

19. Pismo Dyrektora Izby Administracji Skarbowej w Gdańsku nr 2201-IWD.0140.13.2021.2 z dnia 30.04.2021 r.;
20. Pismo Dyrektora Izby Administracji Skarbowej w Gdańsku nr 2201-IWD.0140.15.2021 z dnia 13.05.2021 r.;
21. Pismo Dyrektora Izby Administracji Skarbowej w Gdańsku nr 2201-IWD-0140.2.2022.2 z dnia 12.01.2022 r.;
22. Pismo Dyrektora Izby Administracji Skarbowej w Gdańsku nr 2201-IWD-0140.11.2022.3 z dnia 30.03.2022 r.;
23. Pismo Dyrektora Izby Administracji Skarbowej w Gdańsku nr 2201-IWD-0140.20.2022 z dnia 31.05.2022 r.;
24. Pismo Dyrektora Izby Administracji Skarbowej w Gdańsku nr 2201-IWD.0140.26.2022 z dnia 22.07.2022 r.;
25. Pismo Dyrektora Izby Administracji Skarbowej w Gdańsku nr 2201-IWD-0140.1.2023 z dnia 02.01.2023 r.;
26. Regulaminy organizacyjne Urzędu Skarbowego w Sopocie, obowiązujące w kontrolowanym okresie.

Opis stanu faktycznego:

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

- Pani Dorota Pawłowska – Naczelnik US w Sopocie (02.08.2021 – 30.06.2022)
- Pani Justyna Nowakowska – Naczelnik US w Sopocie (01.07.2022 – 19.02.2023)
- Pani Joanna Trusiewicz – Naczelnik US w Sopocie (od 20.02.2023)

[Dowód: akta kontroli, Q-asystent str. nr 74-79]

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 upoważnień:

- nr 232/2021 z 4 sierpnia 2021,
- nr 281/2022 z 6 lipca 2022,
- nr 79/2023 z 22 lutego 2023,

do wykonywania zadań administratora danych w Urzędzie Skarbowym w Sopocie dla danych, których administratorem jest Dyrektor Izby Administracji Skarbowej w Gdańsku, w zakresie:

a) nadzoru nad bezpieczeństwem przetwarzania danych osobowych,
b) udzielania i odwoływania upoważnień do przetwarzania danych osobowych,
c) zatwierdzania uprawnień do systemów informatycznych,

były odpowiednio:

- Pani Dorota Pawłowska - do 30.06.2022.
- Pani Justyna Nowakowska (01.07.2022 – 19.02.2023)
- Pani Joanna Trusiewicz – od 20.02.2023.

[Dowód: Q-asystent]

Na podstawie Decyzji nr 209 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 Sopocie osobą odpowiedzialną za realizację zadań z zakresu ochrony danych osobowych jest pani **A.P.**, główny specjalista, Wieloosobowe Stanowisko ds. Wsparcia (SWW).

Do zadań pracownika należy w szczególności:

1) 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);
2) weryfikacja upoważnień oraz szkolenie pracowników powracających do pracy po długotrwałej nieobecności;
3) prowadzenie ewidencji szkoleń i ich uczestników;
4) 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);
5) prowadzenie ewidencji osób upoważnionych do przetwarzania danych osobowych;
6) weryfikacja wniosków o nadanie uprawnień do systemów informatycznych pod względem zgodności z upoważnieniem do przetwarzania danych osobowych, a w przypadku akceptacji Zgody na wynoszenie komputera poza miejsce pracy – dodatkowo weryfikacja, czy został załączony podpisany wniosek.
7) 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 Sopocie funkcjonują, zgodnie z Regulaminem organizacyjnym, następujące komórki organizacyjne, na których czele stoją kierownicy działów/referatów/kierujący:

1) SWW – A.P. – kierujący wieloosobowym stanowiskiem;
2) SEW – P.M.– kierownik referatu;
3) SEE – A.D. – kierownik referatu;
4) SER – D.M. – kierownik referatu;
5) SOB – A.L. – kierownik referatu do 31.01.2022 r., od 1.03.2022 r. – M.K. – kierownik referatu;
6) SKA-1 – M.K2– kierownik referatu;
7) SKA-2 – A.M. – kierownik referatu do 31.03.2022 r., od 11.04.2022 r. P.P. – kierownik referatu;
8) SPO – J.G. – kierownik działu, od 20.03.2023 r. - K.K. – p.o. kierownika działu;
9) SKI – M.K3 – kierujący wieloosobowym stanowiskiem;

10) SKK –E.B. –kierujący wieloosobowym stanowiskiem do 31.12.2022 r. a od 1.01.2023 r. centralizacja KKS) p.o. kierownik działu;
a) SKK-1 – D.S. – p.o. kierownik referatu;
b) SKK-2 – E.L. – p.o. kierownik referatu;
c) SKK-3 – M.D. – p.o. kierownik referatu.

Wszyscy kierownicy 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. Kierownik SOB przeprowadził dwa szkolenia nt. ochrony danych osobowych z pracownikami, którzy przez nieuwagę naruszyli tajemnice danych osobowych, 07.09.2022, 11.10.2022 (przesyłka trafiła do innej osoby niż powinna – elektronicznie na portal e-Urząd).

[Dowód: akta kontroli, str. nr 74 – 79, 96 - 116]

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, zabraniem 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 Sopot jest dowodem w aktach kontroli.

[Dowód: akta kontroli, str. nr 53 - 54]

W kontrolowanym okresie nie przeprowadzono kontroli funkcjonalnych.
Naczelnik złożył oświadczenie, w którym opisał swoje działania ws. ochrony danych osobowych. Są to m. in. polecenie przeprowadzania kontroli funkcjonalnych w zakresie przestrzegania zasad „czystego biurka". Wynik ich ma być odnotowywany na karcie „Informacja o przeprowadzonej kontroli funkcjonalnej". Złożono zapotrzebowanie na nowe zamki do szaf z aktami. Przeprowadzono zebranie z pracownikami poświęcone przedmiotowej tematyce.
W kontrolowanym okresie Naczelnik przeprowadził narady poświęcone problematyce ochrony danych i informacji niejawnych.
1) Protokół ze spotkania Naczelnika Urzędu Skarbowego w Sopocie z kierownikami w dniu 13 kwietnia 2022 r.,
2) Protokół ze spotkania Naczelnika Urzędu Skarbowego w Sopocie z kierownikami w dniu 9 maja 2022 r.,
3) Protokół ze spotkania Naczelnika Urzędu Skarbowego w Sopocie z kierownikami w dniu 31 sierpnia 2022 r.,
4) Protokół ze spotkania Naczelnika Urzędu Skarbowego w Sopocie z kierownikami w dniu 13 września 2022 r.,

5) Protokół ze spotkania Naczelnika Urzędu Skarbowego w Sopocie z pracownikami Urzędu w dniu 5 grudnia 2022 r.,
6) Protokół ze spotkania Naczelnika Urzędu Skarbowego w Sopocie z kierownikami i osobami kierującymi w dniu 10 stycznia 2023 r.,
7) Protokół ze spotkania Naczelnika Urzędu Skarbowego w Sopocie z kierownikami i osobami kierującymi w dniu 25 stycznia 2023 r.,

[Dowód: akta kontroli, str. nr 117 - 138]

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:
(...)
Brak uwag.

[Dowód: akta kontroli, str. nr 435-438]

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 68 - 71]

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 zapoznały 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 11 pomieszczeń (1/3 pomieszczeń ogółem), w których zakończono już pracę. W pokoju nr (...) stwierdzono, że jedna z szaf była otwarta (niedomknięta). Na półkach znajdowały się segregatory z aktami zawierającymi dane osobowe. W pozostałych, skontrolowanych pomieszczeniach, naruszenia zasady ochrony fizycznej dokumentów nie stwierdzono.

[Dowód: akta kontroli, str. nr 68 - 71]

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 11 pomieszczeń (1/3 pomieszczeń ogółem), w których zakończono już pracę. W pokoju nr (...) na biurku znajdowała się tzw. koszulka z dokumentami zawierającymi dane osobowe. W pozostałych pokojach nieprawidłowości nie stwierdzono.

[Dowód: akta kontroli, str. nr 68 - 71]

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 68 - 71]

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 11 pomieszczeń (1/3 ogółem). Worki ze ścinkami przechowywane są w zamkniętej, monitorowanej wiacie, na zewnątrz budynku. Naruszeń w/w zasad nie stwierdzono.

[Dowód; akta kontroli, str. nr 68 – 71, 341]

Zestawienie skontrolowanych pomieszczeń.

Lp.	Nr pokoju	Komórka	UWAGI
1.	(...)	SKK-1	Nie stwierdzono nieprawidłowości
2.	(...)	SKK	Dokumenty z danymi pozostawione na biurku (naruszona zasada czystego biurka)
3.	(...)	SKI	Nie stwierdzono nieprawidłowości
4.	(...)	SKA-1	Nie stwierdzono nieprawidłowości
5.	(...)	SKK	Nie stwierdzono nieprawidłowości
6.	(...)	SPO	Nie stwierdzono nieprawidłowości
7.	(...)	SKA-1	Nie stwierdzono nieprawidłowości
8.	(...)	SPO	Jedna otwarta szafa zawierająca dokumenty z danymi (naruszona zasada ochrony fizycznej dokumentów)
9.	(...)	ZN	Sprawdzono zasadę ‘czystego ekranu’ – nie stwierdzono nieprawidłowości
10.	(...)	SEE	Sprawdzono zasadę ‘czystego ekranu’ – nie stwierdzono nieprawidłowości
11.	(...)		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:

- 2201-IWD.0140.15.2020.1 z 21.10.2020 r.
- 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 (30/90 listów). W żadnym przypadku nie stwierdzono naruszenia zasad o których mowa wyżej.
Brak uwag.

{Dowód: akta kontroli, str. nr 341]

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 (CCTV) 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:

- 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. 341]

- Przechowywanie nagrań oraz ich usuwanie,

Zgodnie z oświadczeniem Naczelnika, nagrania z monitoringu usuwane są po upływie 1 – 1,5 miesiąca.
Brak uwag.

[Dowód, akta kontroli, str. nr 343 - 345]

- Udostępnianie nagrań z monitoringu.

W kontrolowanym okresie Naczelnik udostępnił jeden raz nagranie z CCTV. Odbyło się to na wniosek Komendy Miejskiej Policji w (...) z 22.03.2022 r. Nagranie przekazano na nośniku danych (CD). Przekazująca sporządziła stosowny protokół.
Brak uwag.

[Dowód, akta kontroli, str. nr 237 - 239]

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

pomieszczeniach służbowych zajmowanych przez tych pracowników, w zamykanych na klucz szafach. Pozostałe nośniki danych przechowywane są w pomieszczeniu informatyka (pracownik CIRF).
Brak uwag.

[Dowód, akta kontroli, str. nr 343 – 345, 349]

Ustalenia
Kontrolujący stwierdzili jedno naruszenie zasady ochrony fizycznej dokumentów (1/10 skontrolowanych pomieszczeń) oraz jedno naruszenie zasady czystego biurka (1/10 skontrolowanych pomieszczeń).

Działalność Urzędu Skarbowego w Sopocie 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 79/2023 z dnia 22.02.2023 r. do wykonywania zadań administratora danych w Urzędzie Skarbowym w Sopocie;
8. Upoważnienie nr 281/2022 z dnia 06.07.2022 r. do wykonywania zadań administratora danych w Urzędzie Skarbowym w Sopocie;
9. Upoważnienie nr 232/2021 z dnia 04.08.2021 r. do wykonywania zadań administratora danych w Urzędzie Skarbowym w Sopocie;
10. Zarządzenia Dyrektora Izby Administracji Skarbowej w Gdańsku w sprawie wprowadzenia instrukcji „Postępowanie z informacjami stanowiącymi tajemnicę skarbową w Izbie Administracji Skarbowej w Gdańsku”;
11. 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;
12. 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;
13. 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;
14. 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;
15. Pismo Dyrektora Izby Administracji Skarbowej w Gdańsku nr 2201-IWD.0140.15.2020.1 z dnia 21.10.2020 r.;
16. Pismo Dyrektora Izby Administracji Skarbowej w Gdańsku nr 2201-IWD.0140.3.2021.1 z dnia 08.02.2021 r.;
17. Pismo Dyrektora Izby Administracji Skarbowej w Gdańsku nr 2201-IWD.0140.10.2021.1 z dnia 25.03.2021 r.;
18. Pismo Dyrektora Izby Administracji Skarbowej w Gdańsku nr 2201-IWD.0140.13.2021.2 z dnia 30.04.2021 r.;
19. Pismo Dyrektora Izby Administracji Skarbowej w Gdańsku nr 2201-IWD.0140.15.2021 z dnia 13.05.2021 r.;
20. Pismo Dyrektora Izby Administracji Skarbowej w Gdańsku nr 2201-IWD-0140.2.2022.2 z dnia 12.01.2022 r.;

21. Pismo Dyrektora Izby Administracji Skarbowej w Gdańsku nr 2201-IWD-0140.11.2022.3 z dnia 30.03.2022 r.;
22. Pismo Dyrektora Izby Administracji Skarbowej w Gdańsku nr 2201-IWD-0140.20.2022 z dnia 31.05.2022 r.;
23. Pismo Dyrektora Izby Administracji Skarbowej w Gdańsku nr 2201-IWD.0140.26.2022 z dnia 22.07.2022 r.;
24. Pismo Dyrektora Izby Administracji Skarbowej w Gdańsku nr 2201-IWD-0140.1.2023 z dnia 02.01.2023 r.;
25. Regulaminy organizacyjne Urzędu Skarbowego w Sopocie, 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 Sopocie 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 27 marca 2023 r.). Wynika z niego, że na 98 zatrudnionych w US Sopot, z dokumentem zapoznało się 93 osoby, z czego 42 po rozpoczęciu kontroli. 5 osób nie zapoznało się z w/w dokumentem.

[Dowód: akta kontroli, str. nr 90 – 92]

Z Zarządzeniem Dyrektora Izby Administracji Skarbowej nr 45/2020 w sprawie wprowadzenia Polityki Ochrony Danych Osobowych, na 98 zatrudnionych z dokumentem zapoznało się 96 osób, 15 zapoznało się z w/w dokumentem po wszczęciu kontroli. 2 osoby nie zapoznały się (raport z aplikacji Q-asystent z 27 marca 2023 r.).

[Dowód: akta kontroli, str. nr 93 - 95]

Wytyczne DIAS zostały przekazane wszystkim pracownikom za pomocą SZD.

[Dowód: akta kontroli, str. nr 139 - 236]

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 Sopocie osobą odpowiedzialną za realizację zadań z zakresu ochrony danych osobowych jest pani **A.P.**, główny specjalista, Wieloosobowe Stanowisko ds. Wsparcia (SWW). Prowadzi ona ewidencję osób upoważnionych do przetwarzania danych, zgodną ze wzorem opisanym w Procedurze nadawania i odwoływania upoważnień imiennych do przetwarzania danych osobowych (załącznik do Polityki).

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	Uwagi
1.	E. D.	aplikant	01.06.2022	22.06.2022	brak
2.	Ł. W.	aplikant	07.09.2022	28.09.2022	brak
3.	M. W.	stażysta	27.09.2022	30.12.2022	brak
4.	A. W.	stażysta	16.09.2022	15.03.2022	brak
5.	S. Z.	stażysta	16.09.2022	15.03.2023	brak
6.	A. Ć	stażysta	27.09.2022	15.03.2023	brak
7.	J. W.	aplikant	05.12.2022	16.12.2022	brak

Wszystkie z w/w osób zostały przeszkolone z zakresu ochrony danych osobowych na zasadach określonych w SZBI. Uczestnicy szkolenia potwierdzili zapoznanie się z obowiązującymi przepisami oraz zobowiązali się pisemnie do zachowania tajemnicy danych osobowych.
Wszystkim w/w osobom wystawiono w dniu zatrudnienia upoważnienie do przetwarzania danych.
Wobec osób odbywających staż, praktykę, wolontariat, osób kontrolujących, pracowników zleceniowych wygaśnięcie upoważnienia następuje po upływie terminu lub zdarzenia określonego w upoważnieniu i nie wymaga odrębnego wniosku (ust. 6 przedmiotowej procedury).

Brak uwag

[Dowód: akta kontroli, str. nr 52, 249 – 259, 270 - 294]

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.

Kontrolujący sprawdzili, czy wszystkie takie osoby wypełniły przedmiotowe oświadczenie.

Lp.	Imię, nazwisko (inicjały)	Stanowisko	Początek zatrudnienia	Koniec zatrudnienia	Uwagi
1.	M. K.	Ochrona	13.07.2022	trwa	brak
2.	B. Z.	Ochrona	13.07.2022	trwa	brak
3.	G. G.	Personel sprzątający	15.07.2022	trwa	brak
4.	W. B.	Personel sprzątający	15.07.2022	trwa	brak
5.	J. F.	Personel sprzątający	15.07.2022	trwa	brak

Ponadto pracownicy ochrony fizycznej obiektu zostali upoważnieni do przetwarzania danych osobowych przed DIAS. Pracownicy ci obsługują system telewizji przemysłowej (CCTV) (monitoring wizyjny).
Brak uwag.

[Dowód: akta kontroli, str. nr 260 - 269]

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

- wykaz prac remontowych prowadzonych w pomieszczeniach urzędu,
- wykonanych w kontrolowanym okresie archiwizacji i brakowania dokumentów,
- 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 Sopot, w 2022 i 01 – 02.2023 r. przeprowadzono następujące prace remontowe:
(...).

W urzędzie zarchiwizowano 148 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 okresie:
- styczeń, luty, marzec, lipiec, sierpień, wrzesień, październik, grudzień 2022
- styczeń, luty 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 każdych przeprowadzonych remontach. Podobnie, w usługach dotyczących brakowania i archiwizacji dokumentów. W załączeniu przesłano kserokopie przyrzeczeń o zachowaniu poufności.
Ponowne podpisywanie klauzul na miejscu, w urzędzie jest niecelowe.

[Dowód, akta kontroli, str. nr 358 – 359, 364 – 366
385 – 419]

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 Sopocie z obowiązku szkolenia na platformie Atena 2 oraz szkoleń na platformie MOODLE o następującej tematyce.

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

Szkolenia te są obowiązkowe na podstawie wytycznych DIAS, zawartych w pismach, odpowiednio:
Kontrolujący ustalili że na 98 zatrudnionych:

Lp.	Nazwa kursu, platforma szkoleniowa	Ilość osób, które nie odbyły kursu	% ogółu zatrudnionych w US Sopot, którzy odbyli kurs
1.	RODO – Atena 2	19	80,61
2.	Naruszenie ochrony danych - MOODLE	18	81,63
3.	Zasady bezpieczeństwa informacji - MOODLE	6	93,88

[Dowód: akta kontroli, str. nr 55 - 67]

Naczelnik w korespondencji mailowej, na polecenia IOD, zobowiązał pracowników do odbycia szkolenia z zasad bezpieczeństwa informacji (lp. 3 z w/w tabeli). Kierownicy komórek organizacyjnych, tą samą drogą potwierdzili, że podlegli pracownicy takie szkolenia odbyli.

[Dowód, akta kontroli, str. nr 204 – 236]

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 341]

Ustalenia:
Kontrolujący stwierdzili, że do dnia wszczęcia kontroli:

- 15% zatrudnionych nie zapoznało się z Polityką ochrony danych Osobowych IAS w Gdańsku;
- 19% zatrudnionych nie odbyło obowiązkowego szkolenia RODO na platformie Atena-2;
- 18% zatrudnionych nie odbyło obowiązkowego szkolenia „Naruszenie ochrony danych" (platforma MOODLE);
- 6% zatrudnionych nie odbyło obowiązkowego szkolenia „zasady bezpieczeństwa informacji" (platforma MOODLE).

Do pozostałych aspektów działalności Naczelnika w tym zakresie, jako osoby upoważnionej przez Administratora, kontrolujący nie wnoszą uwag.

Ocena cząstkowa:
Działalność Urzędu Skarbowego w Sopocie w zakresie wydawania i unieważniania upoważnień, szkoleń wstępnych, prowadzenia szkoleń w zakresie ochrony danych należy ocenić **pozytywnie z uchybieniami.**

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 79/2023 z dnia 22.02.2023 r. do wykonywania zadań administratora danych w Urzędzie Skarbowym w Sopocie;
8. Upoważnienie nr 281/2022 z dnia 06.07.2022 r. do wykonywania zadań administratora danych w Urzędzie Skarbowym w Sopocie;
9. Upoważnienie nr 232/2021 z dnia 04.08.2021 r. do wykonywania zadań administratora danych w Urzędzie Skarbowym w Sopocie;
10. Zarządzenia Dyrektora Izby Administracji Skarbowej w Gdańsku w sprawie wprowadzenia instrukcji „Postępowanie z informacjami stanowiącymi tajemnicę skarbową w Izbie Administracji Skarbowej w Gdańsku";
11. 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;
12. 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;
13. 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;
14. 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;
15. Pismo Dyrektora Izby Administracji Skarbowej w Gdańsku nr 2201-IWD.0140.15.2020.1 z dnia 21.10.2020 r.;
16. Pismo Dyrektora Izby Administracji Skarbowej w Gdańsku nr 2201-IWD.0140.3.2021.1 z dnia 08.02.2021 r.;
17. Pismo Dyrektora Izby Administracji Skarbowej w Gdańsku nr 2201-IWD.0140.10.2021.1 z dnia 25.03.2021 r.;
18. Pismo Dyrektora Izby Administracji Skarbowej w Gdańsku nr 2201-IWD.0140.13.2021.2 z dnia 30.04.2021 r.;
19. Pismo Dyrektora Izby Administracji Skarbowej w Gdańsku nr 2201-IWD.0140.15.2021 z dnia 13.05.2021 r.;
20. Pismo Dyrektora Izby Administracji Skarbowej w Gdańsku nr 2201-IWD-0140.2.2022.2 z dnia 12.01.2022 r.;
21. Pismo Dyrektora Izby Administracji Skarbowej w Gdańsku nr 2201-IWD-0140.11.2022.3 z dnia 30.03.2022 r.;

22. Pismo Dyrektora Izby Administracji Skarbowej w Gdańsku nr 2201-IWD-0140.20.2022 z dnia 31.05.2022 r.;
23. Pismo Dyrektora Izby Administracji Skarbowej w Gdańsku nr 2201-IWD.0140.26.2022 z dnia 22.07.2022 r.;
24. Pismo Dyrektora Izby Administracji Skarbowej w Gdańsku nr 2201-IWD-0140.1.2023 z dnia 02.01.2023 r.;
25. Regulaminy organizacyjne Urzędu Skarbowego w Sopocie, 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. Naczelnik oświadczył, że kierownicy dokonują przeglądu uprawnień nadanych podległym pracownikom, każdorazowo **w przypadku polecenia IAS w Gdańsku lub Ministerstwa Finansów.**

W 2022 roku dokonali weryfikacji uprawnień na polecenie Działu Bezpieczeństwa i Ochrony Informacji IAS w Gdańsku na podstawie n/w pism:

1. Pismo UNP: 2201-22-001159 z 4.01.2022 r. znak sprawy: 2201-IWO.0140.4.2021.22: weryfikacja uprawnień do: AKADEMIA, Elektroniczna Kontrola Zezwoleń (EKZ), MAB (AFIS),

OWNERS, Platforma Zakupowa eB2B, RoyaltyRange SARP, CRPO – Centralny Rejestr Pełnomocnictw Ogólnych;
Odpowiedź US Sopot: pismo UNP: 2201-22-008665 z 18.01.2022 r.;

2. Pismo UNP: 2201-22-159405 z 17.11.2022 r. znak sprawy: 2201-ICK.4020.2.31.2022: weryfikacja uprawnień w aplikacji WRO-System;
   Dokonano weryfikacji – odpowiedź w tym przypadku nie była wymagana;
3. E-mail z Działu Bezpieczeństwa i Ochrony Informacji IAS Gdańsk z 14.12.2022 r. ws. weryfikacji uprawnień w aplikacji BPS
   Odpowiedź US Sopot: pismo UNP: 2217-22-051568 z 16.12.2022 r. o dokonanej weryfikacji;
4. Pismo UNP: 2201-22-178279 z 23.12.2022 r., znak sprawy: 2201-IWO.041.1.2022.40: systemy teleinformatyczne stosowane w jednostkach organizacyjnych KAS
   Odpowiedź US Sopot: pismo UNP: 2201-22-178666 z 27.12.2022 r.

[Dowód, akta kontroli, str. nr 343 – 345]

Dokonaliśmy weryfikacji terminowości i zasadności nadawania i odbierania uprawnień do wybranych systemów teleinformatycznych oraz blokowania kont domenowych, dla wybranych pracowników US w Sopocie. Są to osoby, które przebywają lub wróciły z długoterminowych nieobecności. W tym celu poprosiliśmy Kierownika Działu IWO o odpowiednie zestawienia z systemu, w którym zaewidencjonowane są takie zdarzenia (SysUp na Portalu Pracownika).
Poniżej zestawienie na podstawie danych otrzymanych z działu IWO:

Lp.	Pracownik	Data nieobecności	Czy zablokowano dostęp do domeny (tak/nie)	Nie odebrane uprawnienia	Uwagi
1.	A.N.	25.04.2022 – 30.09.2022	Nie można stwierdzić jednoznacznie	Legalis, Serwis Ksiąg Wieczystych Ministerstwa Sprawiedliwości, SPBD	Uprawnienie do Systemu Zdalnego Dostępu Resortu Finansów odebrano w X/2022
2.	P.W.	11.08.2022 – 28.12.2022	TAK		Uprawnienia odebrano w II-III/2023
3.	A.K.	01.03.2022 – 30.04.2023	TAK	CRPO, DWP, Legalis, SeRCe KEP, SZD, SZD (z profilem Izby dla pracowników US i UCS)	Nie odebrano uprawnień
4.	A.B.	01.01.2022 - 28.02.2023	TAK	CRPO	Uprawnienia odebrano w V/2022

Lp.	Pracownik	Data nieobecności	Czy zablokowano dostęp do domeny (tak/nie)	Nie odebrane uprawnienia	Uwagi
5.	M.A.	23.07.2021 – 31.12.2022	Nie można stwierdzić jednoznacznie	CEKR/CEKR2	Nie odebrano jednego uprawnienia

[Dowód: akta kontroli, str. nr 51, 343 – 348, 350 - 357]

Zbadaliśmy 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.

Zgodnie z tą instrukcją, 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.

Naczelnik wskazał:

<u>CEPiK (Centralna Ewidencja Pojazdów i Kierowców)</u>

Uprawnienia dostępu do CEPiK są ewidencjonowane w systemie SysUp.

Ścieżka nadawania uprawnień:
Uprawnienia nadawane i odbierane są na wniosek kierownika komórki organizacyjnej. Wniosek w formie papierowej jest podpisywany przez kierownika komórki, następnie przekazywany do podpisu Naczelnika. Skan podpisanego wniosku jest przesyłany przez osobę, która jest administratorem aplikacji CEPiK w urzędzie na adres mailowy: (...) (CIRF). Po nadaniu uprawnień na skrzynkę mailową osoby zgłaszającej przychodzi potwierdzenie nadania/odebrania uprawnień do ww. systemu. Następnie informacja jest odnotowywana przez administratora w systemie SySup.

eKW Serwis Ksiąg Wieczystych Ministerstwa Sprawiedliwości
W systemie SySup można zrobić raport osób, którym zostały nadane uprawnienia do systemu. Z poziomu urzędu nie ma możliwości sprawdzenia dat nadania i odebrania uprawień do ww. systemu.

Rejestr Zastawów Skarbowych (RZS)
Administrator lokalny systemu RZS w tut. urzędzie występuje o dostęp do systemu z poziomu profilu administratora lokalnego w PUE MF. Administrator lokalny może nadawać uprawnienia dla pracowników urzędu na poziomie RZS. Wierzyciel i prowadzi ewidencję osób posiadających dostęp do RZS.

Rejestr Należności Publicznoprawnych (RNP)
Urząd prowadzi wykaz osób w urzędzie, które mają nadane uprawnienia do RNP.
Uprawnienia do tego systemu rejestrowane są i ewidencjonowane przez Naczelnika Trzeciego Urzędu Skarbowego w (…), który jest administratorem centralnym tych rejestrów.

[Dowód, akta kontroli, str. nr 370-380]

Ponadto zapytaliśmy Naczelnika w jaki sposób w urzędzie sprawowany był nadzór nad właściwym wykorzystaniem w/w aplikacji. 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 **nie zwracał** się do właścicieli biznesowych wymienionych aplikacji o wskazane dane, natomiast pracownicy mający do nich dostęp zostali poinformowani przez swoich kierowników o obowiązku korzystania z aplikacji jedynie w celach służbowych.

[Dowód: akta kontroli, str. nr 370 - 380]

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.A.	(...)	24.07.2022 – 31.12.2022
2.	A.B.	(...)	01.01.2022 – 28.02.2023
3.	A.K.	(...)	01.01.2022 – 31.12.2022
4.	A.N.	(...)	25.04.2022 – 30.09.2022
5.	P.W.	(...)	11.08.2022 – 28.12.2022
6.	E.B.	(...)	2022-08-02 - 2022-08-08
7.	D.S.	(...)	2022-06-20 - 2022-07-01
8.	A.D.	(...)	2022-07-18 - 2022-07-29
9.	A.D2	(...)	2022-01-03 - 2022-01-30
10.	M.K.	(...)	2022-01-24 - 2022-01-28
11.	M.K2	(...)	2022-07-11 - 2022-07-31
12.	M.K3	(...)	2022-06-20 - 2022-06-24
13.	E.L.	(...)	2022-02-14 - 2022-02-17
14.	P.M.	(...)	2022-12-12 - 2022-12-16
15.	D.M.	(...)	2022-12-01 - 2022-12-06
16.	P.P.	(...)	2022-03-05 - 2022-03-11
17.	A.P.	(...)	2022-10-05 - 2022-10-07

Odpowiedź Departamentu Poboru Podatków Ministerstwa Finansów brzmi:
W okresach wskazanych w naszym piśmie z 14 kwietnia 2023 roku **nie odnotowano logowań, loginów / zapytań pochodzących od wymienionych osób** do następujących systemów / aplikacji, których jest Właścicielem Biznesowym:

- Scentralizowany System Poboru (SSP),
- aplikacja REMDAT,
- Zintegrowany System Poboru Należności i Rozrachunków z UE i Budżetem (Zefir2),
- Poltax2BPlus,
- Serwis Ksiąg Wieczystych Ministerstwa Sprawiedliwości dla Ministerstwa Finansów,

- Rejestr Należności Publicznoprawnych (RNP).

W okresach wskazanych **nie odnotowano** także logowań wymienionych użytkowników do Systemu Rejestracji Centralnej (SeRCe).
Dodatkowo ustalono, że cztery osoby (które wskazano w załączonym zestawieniu) nie posiadają uprawnień do systemu SeRCe, jako pracownicy Urzędu Skarbowego w Sopocie.
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.

[Dowód: akta kontroli, str. nr 422 - 426]

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 Sopocie 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 wnioskowano o odebranie (zablokowanie)**
1.	P.P.	II Referat SKA	A.K. A.B.	NIE
2.	M.K.	Referat SOB	M.A.	NIE
3.	P.M.	Referat SEW	A.N.	NIE

[Dowód: akta kontroli, str. nr 381 - 384]

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 z pracownika z I Działu Kadr i Administracji Personalnej IAS w Gdańsku brzmi, że nie poinformowano odpowiednich służb o długotrwałych nieobecnościach pracowników.

[Dowód: akta kontroli, str. nr 432 – 434]

O wyjaśnienie sprawy blokowania kont domenowych zapytaliśmy Pana J.K., Kierownika (…).

Otrzymaliśmy odpowiedź, że w korespondencji elektronicznej z lat 2020 – 2023 **nie otrzymał wniosku o konieczności wyłączenia kont wskazanych przez nas osób (M.A., A.B., A.K., A.N., P.W.).**
Nie jest w stanie, na podstawie posiadanych danych, jednoznacznie stwierdzić, czy dostęp do domeny został wyłączony w przypadku dwóch pracownic:

- M.A. – (...)
- A.N. – (...)

Natomiast stwierdził, że n/w pracownice:

- A.B. – (...),
- A.K.– (...),
- P.W. - (...),

w kontrolowanym okresie 2022 i 01 - 02.2023 miały zablokowany dostęp do domeny - po uwzględnieniu informacji „SVC-PS1-001: Konto przeniesione automatycznie w dniu:…" i „LastLogon" -dacie ostatniego logowania.

[Dowód: akta kontroli, str. nr 427 - 431]

Ustalenia:

1. Kierownicy komórek organizacyjnych **nie dokonują**, przynajmniej raz w roku, przeglądu uprawnień do systemów informatycznych podległych pracowników. Takiego przeglądu wymaga Polityka Ochrony danych Osobowych IAS w Gdańsku. Przeglądów takich dokonywali wyłącznie na podstawie poleceń DIAS, tylko w stosunku do wskazanych w pismach systemów. Przegląd w/w uprawnień jest środkiem ochrony danych osobowych od strony poufności, integralności i rozliczalności w aspekcie ochrony danych osobowych.
   Bezpośrednim następstwem tego jest fakt nieodbierania uprawnień do systemów informatycznych długotrwale nieobecnym pracownikom.
2. Uprawnienia do aplikacji zewnętrznych (Elektroniczne Księgi Wieczyste, Rejestr Zastawów Skarbowych, Rejestr Należności Publicznoprawnych) **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.
3. **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.

4. **Kierownicy, nie wnioskowali 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 kluczowej. Takie postępowanie wyklucza możliwość dostępu do ogromnej większości używanych w urzędzie aplikacji. Tymczasem przedstawiciel CIRF nie był w stanie stwierdzić, czy w przypadku dwóch osób taka blokada nastąpiła.

Ocena cząstkowa:
Działalność Urzędu Skarbowego w Sopocie 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 79/2023 z dnia 22.02.2023 r. do wykonywania zadań administratora danych w Urzędzie Skarbowym w Sopocie;
6. Upoważnienie nr 281/2022 z dnia 06.07.2022 r. do wykonywania zadań administratora danych w Urzędzie Skarbowym w Sopocie;
7. Upoważnienie nr 232/2021 z dnia 04.08.2021 r. do wykonywania zadań administratora danych w Urzędzie Skarbowym w Sopocie;
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 Sopocie, 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 skarbowa" (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 skarbowa". Są to głównie materiały przechowywane w Izbie, ale także udostępniane między innymi ministrowi właściwemu do spraw finansów publicznych, Szefowi Krajowej Administracji Skarbowe lub innym organom podatkowym (zgodnie z art. 298 ustawy OP.

Wg oświadczenia Naczelnika, osobą odpowiedzialną za nadzór nad sprawami związanymi Tajemnicą skarbową jest Pani M.K..

W kontrolowanym okresie pracownicy US w Sopocie nie wysyłali i nie otrzymali dokumentów z grupy I (wg I-037/1).

[Dowód: akta kontroli, str. nr 370 - 372]

Kontrolujący sprawdzili prowadzone zapisy w dzienniku ewidencyjnym (DE), w którym rejestrowane jest korespondencja wychodząca i przychodząca z grupy II dokumentów. Wytypowano do sprawdzenia 8 dokumentów na 80 wpisanych w DE.

Brak uwag.

[Dowód: akta kontroli, str. nr 303 – 340]

Sprawdziliśmy ponadto stan zapoznania się pracowników z instrukcją I-037/1.

Brak uwag.

[Dowód: akta kontroli, str. nr 86-89]

Ustalenia:

Naczelnik prawidłowo wykonuje nadzór w obszarze ochrony informacji – tajemnicy skarbowej.

Ocena cząstkowa:
Działalność Urzędu Skarbowego w Sopocie w zakresie ochrony informacji – tajemnicy skarbowej należy ocenić **pozytywnie.**

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. Zobligować podległych pracowników do bezwzględnego zapoznawania się się z dokumentacją Systemu Zarządzania Bezpieczeństwem Informacji (Polityki, Zarządzenia, instrukcje, pisma nadzorcze, etc). Potwierdzenie zapoznania się dokonywać w aplikacji Q-asystent.
4. Egzekwować obowiązkowe szkolenia z ochrony danych (RODO).
5. Dokonywać przynajmniej raz w roku przeglądu uprawnień do systemów informatycznych. (zobowiązani do tego są wszyscy kierownicy komórek organizacyjnych). Czynność tą odpowiednio udokumentować i zarejestrować w SZD (protokół, notatka służbowa).
6. Rejestrować w aplikacji Q-asystent wszystkie uprawnienia do systemów informatycznych (w tym te, których właścicielami biznesowymi są podmioty spoza Krajowej Administracji Skarbowej)
7. Monitorować właściwe wykorzystanie aplikacji (w tym zewnętrznych), przez sprawdzenie 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.
8. Zaplanować 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 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, 24 maja 2023 r.

Dyrektor Izby Administracji Skarbowej w Gdańsku
Barbara Bętkowska - Cela

(kwalifikowany podpis elektroniczny)