



Karpacki Oddział Straży Granicznej
im. 1 Pułku Strzelców Podhalańskich
w Nowym Sączu

Nowy Sącz, dnia 05-07-2022 r.

KA-NK.0910.3.2022 MO

Egz. pojedynczy

pplk SG Tomasz WOJS
Naczelnik
Wydziału Łączności i Informatyki
Karpackiego Oddziału Straży Granicznej

WYSTĄPIENIE POKONTROLNE

Zgodnie z „Planem kontroli przewidzianym do realizacji przez Wydział Kontroli Karpackiego Oddziału Straży Granicznej w 2022 roku”, w Wydziale Łączności i Informatyki KaOSG została przeprowadzona kontrola w trybie zwykłym, na podstawie Decyzji Nr 65 Ministra Spraw Wewnętrznych z dnia 31 maja 2012 r. w sprawie wprowadzenia do stosowania wytycznych w zakresie zasad i trybu przeprowadzania kontroli w urzędach obsługujących organy lub jednostkach organizacyjnych podległych lub nadzorowanych przez Ministra Spraw Wewnętrznych¹, wprowadzonych do stosowania w Straży Granicznej Decyzją Nr 139 Komendanta Głównego Straży Granicznej z dnia 30 sierpnia 2012 r. w sprawie wprowadzenia do stosowania w Straży Granicznej wytycznych w zakresie zasad i trybu przeprowadzania kontroli w urzędach obsługujących organy lub jednostkach organizacyjnych podległych lub nadzorowanych przez Ministra Spraw Wewnętrznych² na temat: „Ochrona danych osobowych w kontekście nadawania upoważnień i uprawnień do przetwarzania danych osobowych w zbiorach danych i systemach teleinformatycznych”.

I. Oznaczenie podmiotu kontrolowanego, jego adres, imię i nazwisko kierownika podmiotu kontrolowanego.

Wydział Łączności i Informatyki
Karpackiego Oddziału Straży Granicznej w Nowym Sączu
im. 1 Pułku Strzelców Podhalańskich,

¹Dz. Urz. Min. Spraw Wew. poz. 43 z późn. zm.

² Dz. Urz. KGSG poz. 47 z późn. zm.

ul. 1 Pułku Strzelców Podhalańskich 5, 33-300 Nowy Sącz.³

Funkcję kierownika podmiotu kontrolowanego w okresie objętym kontrolą pełnił:

- ppłk SG Tomasz Wojs

II. Imię i nazwisko, stanowisko służbowe kontrolerów, nazwa komórki kontroli oraz numer i data upoważnienia do kontroli.

Kierownik zespołu kontrolnego:

- st. chor. szt. SG Marek Olipra – starszy specjalista Wydziału Kontroli,
upoważnienie nr 242/Z/22 z dnia 30 maja 2022 r.⁴

Członek zespołu kontrolnego:

- chor. szt. SG Beata Pasionek – specjalista Wydziału Kontroli,
upoważnienie nr 243/Z/22 z dnia 30 maja 2022 r.⁵

III. Data rozpoczęcia i zakończenia czynności kontrolnych w podmiocie kontrolowanym.

Czynności kontrolne prowadzono w okresie od dnia 30 maja 2022 r. do dnia 15 czerwca 2022 r.

IV. Określenie przedmiotu kontroli i okresu objętego kontrolą.

1. Zakres przedmiotowy kontroli.

Przedmiotem kontroli było stosowanie „Polityki ochrony danych osobowych” w szczególności „Procedury nadawania upoważnień do przetwarzania danych osobowych” w Wydziale Łączności i Informatyki Karpackiego Oddziału Straży Granicznej w Nowym Sączu w zakresie nadawania, zmian i wycofywania upoważnień oraz nadawania i wycofywania uprawnień do przetwarzania danych osobowych w kontekście kryterium legalności, celowości i rzetelności.

2. Cel kontroli.

³Zwany dalej WŁiI.

⁴Akta kontroli karta 6.

⁵Akta kontroli karta 7.

Celem kontroli była ocena przestrzegania „Polityki ochrony danych osobowych” w zakresie nadawania, zmian i wycofywania upoważnień oraz nadawania i wycofania uprawnień do przetwarzania danych osobowych.

3. Okres objęty kontrolą.

Kontrolą objęto okres od dnia 01 lipca 2021 r. do dnia 27 maja 2022 r.

V. Ocena skontrolowanej działalności, ze wskazaniem ustaleń, na których została oparta.

Ocenę skontrolowanej działalności dokonano na podstawie ustalonego stanu faktycznego przy zastosowaniu kryteriów legalności, rzetelności oraz celowości. Dokonano jej na podstawie ustaleń wynikających z otrzymanej od kontrolowanego podmiotu dokumentacji m. in.: upoważnień do przetwarzania danych osobowych, kart „Zleceń nadania dostępu do zbiorów/systemów”, oświadczeń o zapoznaniu się z przepisami i zachowaniu klauzuli poufności i innej dokumentacji dotyczącej zakresu kontroli oraz na podstawie złożonych wyjaśnień przez kierownika podmiotu kontrolowanego.

Pozytywnie z uchybieniami oceniono prowadzenie dokumentacji związanej z przetwarzaniem danych osobowych z uwagi na brak odnotowania w jednym z dwóch szczegółowych zakresów obowiązków i uprawnień zadań Administratora Bezpieczeństwa Zbiorów oraz brak odnotowania w szczegółowym zakresie obowiązków i uprawnień zadań zastępcy Administratora Bezpieczeństwa Zbiorów.

Pozytywnie z uchybieniami oceniono wnioskowanie o nadanie upoważnień, z uwagi na fakt niewłaściwych zaznaczeń w tabeli upoważnień w zakresie kategorii czynności przetwarzania, do których kategorii nie nadano dostępu do zbiorów/systemów lub pomimo nie odznaczenia w karcie upoważnień nadano dostęp w karcie uprawnień do zbioru/systemu.

Odnosząc się do całości kontrolowanego obszaru, zgodnie z przyjętymi kryteriami i miernikami, realizację zadań w WŁiI objętych zakresem kontroli **oceniono pozytywnie z uchybieniami.**

Ocenę sformułowano na podstawie ustaleń przedstawionych poniżej.

W Karpackim Oddziale Straży Granicznej w ramach „Systemu zarządzania bezpieczeństwem informacji” wprowadzono „Politykę ochrony danych osobowych

przetwarzanych w Karpackim Oddziale Straży Granicznej, których administratorem jest Komendant Karpackiego Oddziału Straży Granicznej⁶ z dnia 28.06.2021 r. oraz „Procedurę nadawania upoważnień do przetwarzania danych osobowych w Karpackim Oddziale Straży Granicznej”⁷ z dnia 28.06.2021 r. Dokumenty te obowiązują wszystkich funkcjonariuszy i pracowników KaOSG oraz osoby wykonujące zadania w imieniu lub na zlecenie Administratora KaOSG, niezależnie od podstawy wykonywania tych zadań. Polityka ochrony danych osobowych dotyczy przetwarzania wszystkich danych osobowych, w tym we wszystkich rodzaju rejestrach, skorowidzach, kartotekach, wykazach, listach, księgach, a także w systemach teleinformatycznych użytkowanych w Karpackim Oddziale Straży Granicznej.

Wszystkie osoby w WLiI, które zostały dopuszczone do przetwarzania danych osobowych odbyły szkolenie z zakresu ochrony danych osobowych⁸ oraz zapoznały się z przepisami dotyczącymi ochrony danych osobowych, co zostało potwierdzone poprzez podpisanie *oświadczenia o zapoznaniu się z przepisami i zachowaniu klauzuli poufności*, przy każdorazowym wydaniu im upoważnień.⁹

Zgodnie z „Polityką ochrony” w WLiI wyznaczono Administratora Bezpieczeństwa Zbiorów (ABZ) oraz jego zastępcę. Wykonywanie obowiązków ABZ zostało ujęte w jego szczegółowym zakresie obowiązków i uprawnień dopiero od dnia 12 lipca 2021 r.¹⁰, natomiast wykonywanie obowiązków zastępcy ABZ nie zostało ujęte w jego szczegółowym zakresie obowiązków i uprawnień¹¹. ABZ przechowuje w systemie EZD (Elektroniczne Zarządzanie Dokumentami) upoważnienia oraz zlecenia nadania dostępu do zbiorów/systemów. Wszystkie sprawy związane z wydawaniem/cofaniem upoważnień, nadawaniem i odbieraniem uprawnień zostały zamieszczone we właściwej etykietce. Ponadto kopie przedmiotowej dokumentacji zostały zapisane w formie elektronicznej na dysku twardej komputera użytkowanego przez ABZ. Upoważnienia i uprawnienia były przygotowywane i nadawane w systemie EZD. Powyższe czynności wykonywane były zgodnie z „Polityką ochrony” i z „Procedurą nadawania upoważnień”. Wszystkie „Upoważnienia do przetwarzania danych osobowych” dla osób z WLiI były wydawane na osobnych kartach dla każdej osoby. Ich zmian dokonywano poprzez uchylenie dotychczasowego upoważnienia i wydanie nowego, w którym odnotowywano fakt uchylenia poprzedniego.

⁶ Zwana dalej „Polityką ochrony”.

⁷ Zwana dalej „Procedurą nadawania upoważnień”.

⁸ Akta kontroli karta 10.

⁹ Akta kontroli karty: 12, 19, 26, 29, 33, 38, 45, 52, 59, 70, 81, 89, 99, 104, 109, 116, 121, 125, 132, 135, 139, 148.

¹⁰ Akta kontroli karta 160.

¹¹ Akta kontroli karta 161.

W „Procedurze nadawania upoważnień” szczegółowo określono sposób nadawania upoważnień i uprawnień. W celu wypełnienia obowiązków wynikających z przepisów regulujących przetwarzanie danych osobowych konieczne jest nadanie upoważnień do przetwarzania danych. Natomiast w celu zapewnienia prawidłowego korzystania z systemów TI oraz zbiorów danych osobowych, wprowadza się obowiązek nadawania uprawnień.

Osoby z WLiI realizują zadania służbowe wymagające przetwarzania danych osobowych wynikające z obowiązujących przepisów, jak również z przepisów szczególnych wynikających z dokumentacji dostępu do poszczególnych sieci/systemów zarówno jawnych, jak i niejawnych. Ma to znaczenie w przypadku wyznaczenia osoby z WLiI jako: lokalny administrator, lokalny administrator merytoryczny, lokalny administrator techniczny, lokalny administrator sieci, czy ich dublerzy, ponieważ osoby te oprócz bezpośredniego dostępu do sieci/systemów technicznie administrują oprogramowaniem sieciowym/systemowym bazodanowym, służącym do przetwarzania danych osobowych. Posiadane uprawnienia jako w/w administratorzy bądź ich dublerzy do poszczególnych sieci/systemów sprowadzają się do utrzymania ciągłości działania i utrzymania dostępności systemów (technicznego administrowania siecią) na poziomie całej jednostki. Osoby te zostały prawidłowo wskazane w Wykazie ATI prowadzonym w WOI KaOSG.

W wielu przypadkach posiadane uprawnienia do sieci/systemów nie mają żadnego odpowiednika w arkuszu Rejestru Czynności w upoważnieniach, niemniej powinny być uwzględnione w zakresie danych na karcie uprawnień. Wynika to ze stanowiska naczelnika WOI KaOSG, które zostało sformułowane przy jednej z poprzednich kontroli o tożsamym zakresie (...) *fakt, że nadawanie dostępu do zbiorów/systemów, które nie są uwzględnione w Rejestrach czynności, ale są wykorzystywane w realizacji zadań służbowych lub też służą dostępem do danych archiwalnych, podyktowane jest monitorowaniem zakresów uprawnień dostępowych tak, aby można było kontrolować dostęp do systemów w momencie zmiany stanowiska służbowego czy też zakończenia stosunku służbowego (...)*. Z uwagi na to, że systemy niejawne podlegają pod ustawę o ochronie informacji niejawnej, osobom z WLiI, które posiadały wpisy o uprawnieniach (nadanie) do sieci/systemów niejawnych jako lokalni administratorzy, zostały one wykreślone (odebrane) mimo, że osoby te fizycznie dalej administrują daną siecią/systemem¹². Osoby te zostały prawidłowo wskazane w wykazie prowadzonym w WOI KaOSG. W powyższej kwestii wyjaśnienia złożył naczelnik WLiI, który stwierdził „(...) osoby pełniące funkcję określone w dokumentacjach do systemów niejawnych (...) z zaleceń WOI wpisywane były uprawnienia wynikające z dokumentacji

¹² Akta kontroli karta 175.

systemów do „zlecenie/nadania dostępu do zbiorów/systemów” w chwili obecnej administrowanie systemami/sieciami NIEJAWNYMI określone jest decyzją nr 136 KaOSG z dnia 18 września 2018 roku (...). Rodzaj administracji (lokalny, techniczny, itp.) określony jest w dokumentacji bezpieczeństwa danego systemu/sieci”.¹³ Potwierdził powyższe również naczelnik WOI KaOSG w przesłanej odpowiedzi „(...) administratorzy (...) przetwarzają dane osobowe w zależności od systemu TI. Dokumentacja bezpieczeństwa poszczególnych systemów określa sposób przetwarzania danych (...) odwołanie bądź powołanie administratorów powinno odbywać się każdorazowo poprzez składania wniosków na podstawie D_136 komendanta KaOSG z dnia 18.09.2018 r.”.¹⁴

W skontrolowanych upoważnieniach 21 osobom z WŁiI nadano upoważnienia w zakresie kategorii czynności przetwarzania danych 18/RCP/KaOSG - „Serwisowanie sprzętu teleinformatycznego” nie nadając w karcie uprawnień dostępu do zbiorów/systemów. Z wyjaśnień naczelnika WŁiI na powyższe wynika, że „nadany w upoważnieniu dostęp do zbioru 18/RCP/KaOSG (...) jest niezbędne do wykonywania czynności serwisowych sprzętu informatyki, a brak na karcie uprawnień związanych jest z brakiem w rejestrze numeru zbiorów danych osobowych odpowiadającej tej kategorii”.¹⁵ Potwierdził to również naczelnik WOI w przesłanym stanowisku „(...) czynność przetwarzania (...) jest czynnością bez przypisanego zbioru danych. Przetwarzanie danych odbywać się może w momencie jakichkolwiek operacji związanych z serwisowaniem sprzętu TI / zdalny dostęp do komputera/ (...)”¹⁶. Powyższe wyjaśnienia zostały uwzględnione.

W skontrolowanych upoważnieniach 10 osobom z WŁiI nadano upoważnienia w zakresie kategorii czynności przetwarzania danych 2/RCP/KaOSG - „Obsługa kadrowa” nie nadając w karcie uprawnień dostępu do zbiorów/systemów odpowiadających tej kategorii. W 4 przypadkach nadano upoważnienia w zakresie czynności przetwarzania danych 1/WKC/KGSG - „Ochrona granicy państwowej i kontrola ruchu granicznego” nie nadając w karcie uprawnień dostępu do zbiorów systemów odpowiadających tej kategorii. W jednym przypadku nadano upoważnienie w zakresie kategorii czynności przetwarzania danych 4/RCP/KGSG - „Obsługa logistyczna” zamiast 12/RCP/KaOSG - „Obsługa logistyczna”. Z wyjaśnień naczelnika WŁiI na powyższe wynika, że „wkrały się błędnie zaznaczone zbiory danych (...) omyłkowo nadano dostęp do zbioru”¹⁷.

¹³ Akta kontroli karta 170.

¹⁴ Akta kontroli karta 174.

¹⁵ Akta kontroli karta 170.

¹⁶ Akta kontroli karta 174.

¹⁷ Akta kontroli karta 170.

W 4 przypadkach w „Zleceniu nadania dostępu do zbiorów/systemów” nadano uprawnienie do systemu „Logistyka (Karpacki Oddział Straży Granicznej)”, natomiast w upoważnieniach do przetwarzania danych osobowych brak jest zaznaczenia numeru arkusza Rejestru Czynności uprawniającego do wglądu we wskazane czynności rejestru. W związku z powyższym naczelnik WLiI złożył stosowne wyjaśnienia, w których napisał, że „omyłkowo nadano dostęp do zbioru”¹⁸.

W jednym przypadku w „Zleceniu nadania dostępu do zbiorów/systemów” odebrano dwa uprawnienia nie wycofując dwóch stosownych wpisów w arkuszu Rejestru Czynności w upoważnieniu. Naczelnik WLiI wyjaśnił, że „arkusze rejestru czynności zostały usunięte z Wykazu zbiorów danych osobowych przetwarzanych w Straży Granicznej, których administratorem jest Komendant Główny Straży Granicznej, a Upoważnienie nie zostało zaktualizowane”.¹⁹

W jednym przypadku numer upoważnienia nie był zgodny z numerem w „Zleceniu nadania dostępu do zbiorów/systemów” co zostało wytłumaczone jako pomyłka pisarska w przepisywaniu numeru upoważnienia na numer zlecenia nadania dostępu. W jednym przypadku w „Zleceniu nadania dostępu do zbiorów/systemów” został pominięty numer z upoważnienia.

Powyższe zostało ocenione jako uchybienia, gdyż te odstępstwa od stanu pożądanego miały wyłącznie charakter formalny nie powodujący negatywnych następstw dla kontrolowanej działalności.

Obszar oceniono pozytywnie z uchybieniami.

VI. Zakres, przyczyny i skutki stwierdzonych nieprawidłowości oraz wskazanie osób za nie odpowiedzialnych.

W kontrolowanym podmiocie w zakresie przedmiotowym kontroli nie stwierdzono nieprawidłowości.

VII. Zalecenia i wnioski pokontrolne.

1. Dokonać analizy wydanych upoważnień i nadanych uprawnień, a następnie dokonać stosownych zmian wynikających z przeprowadzonej kontroli.

¹⁸ Akta kontroli karta 170.

¹⁹ Akta kontroli karta 170.

2. Uzupelnic szczegolowy zakres obowiazkow i uprawnień zastępcy ABZ o stosowny zapis.

VIII. Wystąpienie pokontrolne sporządzono w egzemplarzu pojedynczym, który kierownikowi podmiotu kontrolowanego zostanie udostępniony w EZD.

IX. Fakt przeprowadzenia kontroli odnotowano w książce kontroli Karpackiego Oddziału Straży Granicznej, zarejestrowanej pod numerem Rtd nr 33/2016, na karcie 35, poz. 4.

X. Informację o wykonaniu zaleceń lub wykorzystaniu wniosków, a także o podjętych działaniach lub przyczynach ich niepodjęcia należy przedłożyć zarządzającemu kontrolę w terminie| do 20 sierpnia 2022 r. za pośrednictwem Naczelnika Wydziału Kontroli.

Z poważaniem

K O M E N D A N T

Karpackiego Oddziału Straży Granicznej

w Nowym Sączu

w z. Zastępcy Komendanta

płk SG Renata Obrzut

podpisano elektronicznie certyfikatem PKI SG