Komenda Główna Straży Granicznej
Biuro Ochrony Informacji Niejawnych
02-514 Warszawa Al. Niepodległości 100

Warszawa dnia 07.06.08. 2011 r.

Informacja z kontroli przeprowadzonej w Nadodrzańskim Oddziale Straży Granicznej w terminie od dnia 12.04.2011 r. do dnia 10.06.2011 r.

Na podstawie § 4 pkt 6 Zarządzenia Nr 11 Ministra Spraw Wewnętrznych i Administracji z dnia 02 czerwca 2010 r. w sprawie szczegółowych zasad i trybu przeprowadzania kontroli przez Ministra Spraw Wewnętrznych i Administracji oraz organy i jednostki organizacyjne podległe lub nadzorowane przez Ministra Spraw Wewnętrznych i Administracji (Dz. Urz. MSWiA Nr 7, poz. 29 oraz Nr 9, poz. 44), zwanego dalej „Zarządzeniem Nr 11", w związku z ustawą z dnia 29.08.1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926 ze zm.) Biuro Ochrony Informacji Niejawnych KGSG, przeprowadziło w dniach 12.04.2011 r. - 10.06.2011 r. w Nadodrzańskim Oddziale Straży Granicznej (NoOSG) kontrolę problemową w zakresie „Kontrola zastosowanych środków technicznych i organizacyjnych zapewniających ochronę danych osobowych przetwarzanych w dokumentacji medycznej, profilaktycznej i psychologicznej w Nadodrzańskim Oddziale Straży Granicznej".

Zarządzającym kontrolę był, z upoważnienia Komendanta Głównego Straży Granicznej, Dyrektor Biura Ochrony Informacji Niejawnych Komendy Głównej Straży Granicznej – płk SG Krzysztof Gawęda.

Okres objęty kontrolą: od dnia 01.01.2010 r. do dnia 10.06.2011 r.

W okresie objętym kontrolą, kierownikiem podmiotu kontrolowanego był:

a) od dnia 01.01.2010 r. do dnia 11.04.2011 r. - płk SG Jarosław Frączyk,

b) od dnia 12.04.2011 r. – płk SG Michał Kogut.

Kontrolę przeprowadził zespół w składzie:

Kierownik zespołu kontrolnego:

płk SG Grzegorz Wieczorek - radca w Biurze Ochrony Informacji Niejawnych Komendy Głównej Straży Granicznej,

Członkowie zespołu kontrolnego:

- kpt. SG Anna Ilcewicz - starszy asystent Wydziału I Archiwum Straży Granicznej Biura Ochrony Informacji Niejawnych Komendy Głównej Straży Granicznej,
- ppor. SG Jolanta Bilińska - ekspert Wydziału Bezpieczeństwa Teleinformatycznego i Ochrony Danych Osobowych Biura Ochrony Informacji Niejawnych Komendy Głównej Straży Granicznej,

- ppor. SG Michał Zapalski - starszy specjalista Wydziału Bezpieczeństwa Teleinformatycznego i Ochrony Danych Osobowych Biura Ochrony Informacji Niejawnych Komendy Głównej Straży Granicznej.

Wyniki kontroli zostały przedstawione w protokole kontroli podpisanym przez zespół kontrolny i kierownika podmiotu kontrolowanego oraz w wystąpieniu pokontrolnym przesłanym kierownikowi podmiotu kontrolowanego.

W ramach przeprowadzonych czynności kontrolnych zespół kontrolny dokonał kontroli zastosowanych środków organizacyjnych i technicznych zapewniających ochronę danych osobowych przetwarzanych w dokumentacji medycznej, profilaktycznej i psychologicznej w NoOSG poprzez sprawdzenie:

1) sporządzonego przez Komendanta Nadodrzańskiego Oddziału Straży Granicznej zestawienia zbiorów, w których funkcjonariusze i pracownicy Nadodrzańskiego Oddziału Straży Granicznej przetwarzają dane osobowe, z wykazem zbiorów danych osobowych;
2) opracowania przez Komendanta Nadodrzańskiego Oddziału Straży Granicznej dokumentacji opisującej sposób przetwarzania danych oraz zastosowanych środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych;
3) sposobu postępowania z dokumentacją zawierającą dane osobowe zawarte w dokumentacji medycznej, profilaktycznej i psychologicznej, w tym sposobu zabezpieczenia budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym są one przetwarzane;
4) posiadania przez funkcjonariuszy i pracowników upoważnień do przetwarzania danych osobowych;
5) sposobu realizacji prawa dostępu osób w trybie art. 32 i 33 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych;
6) stopnia znajomości zasad postępowania z dokumentami zawierającymi dane osobowe, w szczególności znajomości dokumentacji - Polityki bezpieczeństwa przetwarzania danych osobowych i Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, przez osoby przetwarzające dane osobowe;
7) sposobu udostępniania danych osobowych;
8) sposobu zabezpieczenia wybranych stanowisk komputerowych, na których przetwarzane są dane osobowe zgodnie z obowiązującymi przepisami, w tym rozporządzeniem Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych i Instrukcją zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.

Po przeprowadzeniu kontroli zespół kontrolny ocenił pozytywnie z zastrzeżeniami skontrolowaną działalność w NoOSG, z uwagi na fakt, że nie wystąpiły przesłanki oceny negatywnej, a stwierdzone nieprawidłowości nie miały zasadniczego wpływu na ochronę danych osobowych.

Sformułowana ocena wynika z następujących ustaleń kontroli:

1. W zakresie zbiorów danych, w których funkcjonariusze i pracownicy NoOSG przetwarzają dane osobowe:

   Zespół kontrolny stwierdził, iż wskazane przez Komendanta NoOSG, w sporządzonych zestawieniach, zbiory danych, w których funkcjonariusze i pracownicy NoOSG przetwarzają dane osobowe, są zgodne z „Wykazem zbiorów danych osobowych, których administratorem jest Komendant Główny Straży Granicznej" oraz z „Wykazem zbiorów danych osobowych, których administratorem jest Komendant Nadodrzańskiego Oddziału Straży Granicznej" wraz z Aneksami do „Wykazu zbiorów danych osobowych, których administratorem jest Komendant Nadodrzańskiego Oddziału Straży Granicznej".

   Niemniej jednak zespół kontrolny stwierdził, iż „Wykaz zbiorów danych osobowych, których administratorem jest Komendant Nadodrzańskiego Oddziału Straży Granicznej" jako podstawy prawne prowadzenia zbiorów przywołują akty prawne rangi rozporządzeń.

   Zgodnie z art. 27 ust. 2 pkt 2 i 6 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych przetwarzanie danych tzw. „szczególnie chronionych" jest dopuszczalne na podstawie ustawy. Dlatego też, w odniesieniu do zbiorów danych, w których przetwarzane są dane, o których mowa w art. 27 ust. 1 ustawy, w kolumnie „Podstawa prawna utworzenia zbioru", obok przywołanych już rozporządzeń, należy wymienić również akt prawny rangi ustawowej.

   Ponadto, do kontroli przedstawiono Książkę przyjęć ambulatoryjnych, w której gromadzone są następujące dane: data przyjęcia, imię i nazwisko pacjenta oraz swobodne skróty (zapiski) lekarza. W ocenie zespołu kontrolnego przedstawione dane stanowią dane osobowe w myśl art. 6 ust. 1 ustawy z dnia 29.08.1997 r. o ochronie danych osobowych, gdyż za dane osobowe uważa się cyt. „wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej".

   W konsekwencji przedmiotową Książkę należy uznać za odrębny zbiór danych lub element wchodzący w skład innego zbioru.

2. W zakresie posiadania przez funkcjonariuszy i pracowników upoważnień do przetwarzania danych osobowych:

   Zespół kontrolny dokonał sprawdzenia posiadania upoważnień do przetwarzania danych osobowych przez wybrane osoby wskazane w sporządzonych przez Komendanta NoOSG zestawieniach, jako osoby przetwarzające dane osobowe w zakresie dotyczącym kontroli. Przedłożone zespołowi kontrolnemu upoważnienia do przetwarzania danych osobowych uprawniają wymienione w nich osoby do przetwarzania danych osobowych w zakresie, w jakim zostały one wydane.

   Wszyscy skontrolowani funkcjonariusze i pracownicy przetwarzający dane osobowe w kontrolowanym zakresie posiadają upoważnienia do przetwarzania danych osobowych.

3. W zakresie sposobu udostępniania danych osobowych oraz realizacji prawa dostępu osób w trybie art. 32 i 33 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. z 2002 r., Nr 101 poz. 926 ze zm.):

   Zespół kontrolny ustalił, że dane osobowe, ze zbiorów danych w zakresie dotyczącym dokumentacji medycznej, profilaktycznej i psychologicznej, nie były udostępniane w

trybie art. 32 i 33 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (nie odnotowano żadnych spraw).

4. W zakresie stopnia znajomości zasad postępowania z dokumentami zawierającymi dane osobowe, w szczególności znajomości dokumentacji - Polityki bezpieczeństwa przetwarzania danych osobowych i Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, przez osoby przetwarzające dane osobowe:

   Na podstawie uzyskanych odpowiedzi na kierowane do wybranych osób pytania dotyczące znajomości zasad określonych w przepisach o ochronie danych osobowych, zespół kontrolny ustalił, że pytane osoby znają zasady postępowania z dokumentami zawierającymi dane osobowe, a w szczególności znają przepisy Polityki bezpieczeństwa przetwarzania danych osobowych i Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.

5. W zakresie sposobu zabezpieczenia wybranych stanowisk komputerowych, na których przetwarzane są dane osobowe zgodnie z obowiązującymi przepisami, w tym rozporządzeniem Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz.U. Nr 100, poz. 1024) i Instrukcją zarządzania systemem informatycznym służącym do przetwarzania danych osobowych:

   W trakcie czynności kontrolnych zespół kontrolny ustalił, że przetwarzanie danych osobowych w ramach dokumentacji medycznej, profilaktycznej i psychologicznej odbywa się przy wykorzystaniu systemów teleinformatycznych.

   Zespół kontrolny stwierdził, że skontrolowane stanowiska komputerowe, zabezpieczone są zgodnie z obowiązującymi przepisami, w tym rozporządzeniem Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz.U. Nr 100, poz. 1024) i Instrukcją zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.

   Niemniej jednak stwierdzono, iż na jednym komputerze system operacyjny umożliwia uwierzytelnienie użytkownika, który, nigdy nie wykorzystywał i nie wykorzystuje konta na tym komputerze oraz nie zna hasła używanego do uwierzytelnienia. W ocenie zespołu kontrolnego, biorąc pod uwagę ogólne zasady bezpieczeństwa, nie jest zasadnym utrzymywanie profilu użytkownika, który nie wykorzystuje stanowiska komputerowego.

6. W zakresie sposobu postępowania z dokumentacją zawierającą dane osobowe zawarte w dokumentacji medycznej, profilaktycznej i psychologicznej, w tym sposobu zabezpieczenia budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym są one przetwarzane:

   Po dokonaniu sprawdzenia sposobu postępowania z dokumentacją zawierającą dane osobowe pochodzące z dokumentacji medycznej, profilaktycznej i psychologicznej, w tym sposobu zabezpieczenia budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym są one przetwarzane, zespół kontrolny ustalił, że sposób

przetwarzania danych oraz obiegu informacji w odniesieniu do zbioru danych Akta postępowań powypadkowych oraz dokumentacji z badań psychologicznych jest niezgodny z § 17 i 18 decyzji Nr 59 Komendanta Głównego Straży Granicznej z dnia 25.02.2010 r. w sprawie wprowadzenia instrukcji kancelaryjnej w Straży Granicznej oraz art. 38 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, ponieważ nie wszystkie dokumenty gromadzone w ramach prowadzonego postępowania powypadkowego są ewidencjonowane oraz nie wszystkie dokumenty wchodzące w skład dokumentacji z przeprowadzonego badania psychologicznego nie podlegają szczegółowej ewidencji, w wyniku czego nie ma możliwości zweryfikowania, a więc i rozliczenia, jakie dokumenty i w jakiej ilości stron wchodzą w skład wymienionej dokumentacji.

Ponadto zespół kontrolny w ramach kontroli sposobu włączenia do akt osobowych wyników ocen, opinii psychologicznych oraz sprawozdań z badań psychofizjologicznych w wybranych Teczkach akt osobowych, stwierdził, różnorodny sposób zabezpieczenia kopert, co jak wynika z oświadczenia Naczelnika WKiSz NoOSG, jest warunkowane brakiem ogólnych, centralnych ujednoliconych zasad w Straży Granicznej zasad w przedmiotowym zakresie.

Z uwagi na powyższe oceny i ustalenia, zespół kontrolny wniósł o realizację niżej wymienionych wniosków:

1. W „Wykazie zbiorów danych osobowych, których administratorem jest Komendant Nadodrzańskiego Oddziału Straży Granicznej", w odniesieniu do zbiorów danych, w których przetwarzane są dane, o których mowa w art. 27 ust. 1 ustawy, w kolumnie „Podstawa prawna utworzenia zbioru" przywołać akt prawny rangi ustawowej obok przywołanych już rozporządzeń.
2. Książkę przyjęć ambulatoryjnych uznać za odrębny zbiór danych lub jako element wchodzący w skład innego zbioru.
3. Zastosować, w odniesieniu do dokumentów przetwarzanych w ramach dokumentacji Akta postępowań powypadkowych oraz dokumentacji z badań psychologicznych wymaganie wynikające z § 17 i 18 decyzji Nr 59 Komendanta Głównego Straży Granicznej z dnia 25.02.2010 r. w sprawie wprowadzenia instrukcji kancelaryjnej w Straży Granicznej w związku z art. 38 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych pozwalające na możliwość zweryfikowania, a więc i rozliczenia, jakie dokumenty i w jakiej ilości stron wchodzą w skład wymienionej dokumentacji.
4. Opracować, w uzgodnieniu z dyrektorem BKiSzk KGSG, wzorcowy i jednolity sposób włączania do akt osobowych ocen, opinii psychologicznych oraz sprawozdań z badań psychofizjologicznych.
5. Dokonać analizy w zakresie zasadności utrzymania na komputerze konta użytkownika, który nie wykorzystuje stanowiska komputerowego.

Kierownik zespołu kontrolnego
płk SG Grzegorz Wieczorek