

BIURO GIODO
Departament Inspekcji

Zestawienie wyników kontroli (sektorowych)

zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych, które zostały przeprowadzone w 2015 r. przez inspektorów Biura GIODO w organach mających bezpośredni dostęp do Wizowego Systemu Informacyjnego (VIS) poprzez Krajowy System Informatyczny (KSI)

Zakres kontroli: dane osobowe przetwarzane w związku z dostępem do Krajowego Systemu Informatycznego w celu dokonywania wpisów danych VIS oraz wglądu do danych VIS, w następującym zakresie:

1. Ustalenie sposobu realizacji uprawnienia do bezpośredniego dostępu do Krajowego Systemu Informatycznego w celu dokonywania wpisów danych VIS (art. 5 ust. 1 ustawy o udziale Rzeczypospolitej Polskiej w Systemie Informacji Schengen oraz Wizowym Systemie Informacyjnym). Ustalenie sposobu realizacji uprawnienia do bezpośredniego dostępu do Krajowego Systemu Informatycznego w celu wglądu do danych VIS (art. 6 ustawy o udziale Rzeczypospolitej Polskiej w Systemie Informacji Schengen oraz Wizowym Systemie Informacyjnym).
2. Ustalenie, czy realizowany jest obowiązek informacyjny, o którym mowa w art. 37 rozporządzenia Parlamentu Europejskiego i Rady (WE) nr 767/2008 z dnia 9 lipca 2008 r. w sprawie Wizowego Systemu Informacyjnego (VIS) oraz wymiany danych pomiędzy państwami członkowskimi na temat wiz krótkoterminowych (rozporządzenie w sprawie VIS) względem osób ubiegających się o wizę oraz osób, o których mowa w art. 9 ust. 4 lit f ww. rozporządzenia oraz czy wdrożono odpowiednie procedury w zakresie realizacji praw osób, których dane dotyczą.
3. Ustalenie, w jaki sposób zapewnia się, aby wpisy danych VIS były zgodne z prawem, a ponadto, aby dane VIS były dokładne i aktualne (art. 5 ust. 2 pkt 2 ustawy o udziale Rzeczypospolitej Polskiej w Systemie Informacji Schengen oraz Wizowym Systemie Informacyjnym).

4. Ustalenie, w jaki sposób zapewnia się usuwanie danych VIS po upływie okresu, na który dane te zostały wprowadzone (art. 5 ust. 2 pkt 3 ustawy o udziale Rzeczypospolitej Polskiej w Systemie Informacji Schengen oraz Wizowym Systemie Informacyjnym).
5. Ustalenie sposobu informowania centralnego organu technicznego KSI o ujawnionych nieprawidłowościach w związku z wykorzystaniem danych VIS poprzez Krajowy System Informatyczny (art. 5 ust. 2 pkt 4 ustawy o udziale Rzeczypospolitej Polskiej w Systemie Informacji Schengen oraz Wizowym Systemie Informacyjnym).
6. Ustalenie sposobu rozpatrywania wniosków Państw Członkowskich o dokonanie zmiany lub usunięcie danych VIS wprowadzonych przez dany organ oraz powiadomienia Państw Członkowskich o konieczności dokonania zmiany lub usunięcia danych VIS wprowadzonych przez te Państwa Członkowskie (art. 5 ust. 2 pkt 5 ustawy o udziale Rzeczypospolitej Polskiej w Systemie Informacji Schengen oraz Wizowym Systemie Informacyjnym).
7. Ustalenie, czy zostały opracowane procedury kontrolne wskazujące działania mające na celu zapewnienie zgodności wykorzystywania danych z obowiązującymi przepisami (art. 24 ustawy o udziale Rzeczypospolitej Polskiej w Systemie Informacji Schengen oraz Wizowym Systemie Informacyjnym).
8. Ustalenie, czy wszystkie osoby mające dostęp do danych VIS zostały przeszkolone z zakresu bezpieczeństwa i ochrony danych (art. 25 ust. 1 ustawy o udziale Rzeczypospolitej Polskiej w Systemie Informacji Schengen oraz Wizowym Systemie Informacyjnym).
9. Ustalenie, czy wszystkim osobom mającym dostęp do danych VIS zostały nadane upoważnienia do dostępu do Krajowego Systemu Informatycznego (KSI) oraz wykorzystywania danych (art. 25 ust. 2 ustawy o udziale Rzeczypospolitej Polskiej w Systemie Informacji Schengen oraz Wizowym Systemie Informacyjnym).
10. Czy zostały zastosowane przez administratora danych środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności, czy ww. administrator danych zabezpieczył dane przed ich udostępnieniem osobom nieupoważnionym, zabranieniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem (art. 36 ust. 1 ustawy o ochronie danych osobowych).
11. Czy administrator danych prowadzi dokumentację opisującą sposób przetwarzania danych oraz środki, o których mowa w art. 36 ust. 1 ustawy (art. 36 ust. 2 ustawy o ochronie danych osobowych).

12. Czy administrator danych powołał administratora bezpieczeństwa informacji (art. 36a ust. 1 ustawy o ochronie danych osobowych).
13. W jaki sposób realizowany jest obowiązek zapewnienia kontroli nad tym, jakie dane osobowe, kiedy i przez kogo zostały do zbioru wprowadzone oraz komu są przekazywane (art. 38 ustawy o ochronie danych osobowych).
14. Czy prowadzona jest ewidencja osób upoważnionych do przetwarzania danych zgodnie z art. 39 ustawy o ochronie danych osobowych.
15. Kontrola systemów informatycznych w zakresie spełnienia wymogów określonych w rozporządzeniu 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).

Cele kontroli: ustalenie zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych przez organy posiadające bezpośredni dostęp do Wizowego Systemu Informacyjnego realizowany poprzez Krajowy System Informatyczny (KSI), umożliwiającą wgląd w dane VIS oraz dokonywanie wpisów danych VIS.

Czynności kontrolne przeprowadzono w okresie od maja 2015 r. do grudnia 2015 r.

Kontrole zostały podjęte z inicjatywy własnej Generalnego Inspektora Ochrony Danych Osobowych na podstawie harmonogramu kontroli sektorowych na 2015 r.

Kontrole zostały przeprowadzone w: Ministerstwie Spraw Zagranicznych (1 kontrola), Komendzie Głównej Straży Granicznej (1 kontrola), jednostce Straży Granicznej (1 kontrola), w wydziałach konsularnych przy ambasadach Rzeczypospolitej Polskiej (4 kontrole) oraz w Urzędzie do Spraw Cudzoziemców (1 kontrola).

Wyniki kontroli:

1. Na podstawie kontroli przeprowadzonej przez inspektorów Biura Generalnego Inspektora Ochrony Danych Osobowych w Ministerstwie Spraw Zagranicznych stwierdzono uchybienia w procesie przetwarzania danych osobowych, które polegały na:

1) nieuwzględnieniu w dokumentacji opisującej proces przetwarzania danych części punktów wizowych, w których są przyjmowane od interesantów wnioski wizowe oraz niewskazaniu aktualnego adresu wydziału konsularnego jednej z ambasad RP, co stanowiło naruszenie § 4 pkt 1 rozporządzenia,

2) nieuwzględnieniu systemów informatycznych WWW SIS oraz WWW VIS w wykazie zbiorów danych osobowych, stanowiącym załącznik do polityki bezpieczeństwa danych osobowych, co stanowiło naruszenie § 4 pkt 2 rozporządzenia.

W związku ze stwierdzeniem ww. uchybień Generalny Inspektor zwrócił się do Ministra Spraw Zagranicznych o złożenie wyjaśnień w powyższym zakresie i przesłanie dowodów potwierdzających usunięcie powyższych uchybień.

2. W jednym z poddanych kontroli wydziałów konsularnych stwierdzono uchybienie polegające na nieuwzględnieniu w dokumentacji opisującej proces przetwarzania danych - punktów wizowych, gdzie są przyjmowane od interesantów wnioski wizowe, stanowiących obszar przetwarzania danych osobowych.

Wobec powyższego Generalny Inspektor Ochrony Danych Osobowych zwrócił się do Ministra Spraw Zagranicznych o złożenie wyjaśnień w ww. zakresie i przesłanie dowodów potwierdzających usunięcie powyższych uchybień.

3. W toku kontroli przeprowadzonej w placówce Straży Granicznej ustalono, że procedury kontrolne wskazujące działania podejmowane w ramach Straży Granicznej mające na celu zapewnienie zgodności wykorzystania danych VIS z obowiązującymi przepisami funkcjonują w oddziale Straży Granicznej, któremu placówka podlega oraz w Komendzie Głównej Straży Granicznej. Dostęp do logów systemu informatycznego dotyczących aktywności użytkowników tego systemu, w tym aktywności związanych z wykorzystaniem danych VIS, posiadają pracownicy Komendy Głównej Straży Granicznej. Komenda Główna Straży Granicznej może występować do Centralnego Organu Technicznego KSI o udostępnienie logów z aplikacji WWW VIS i WWW SIS, dotyczących działań podejmowanych przez funkcjonariuszy i pracowników cywilnych skontrolowanej placówki SG w tych aplikacjach. Ustalono, że poddana kontroli placówka SG nie występowała do tej pory o udostępnienie tych logów.

W związku z powyższym, w celu sprawdzenia, w jaki sposób zapewniona jest kontrola nad tym, jakie dane osobowe, kiedy i przez kogo zostały do zbioru wprowadzone oraz komu są przekazywane oraz w celu ustalenia obowiązujących procedur kontrolnych wskazujących działania podejmowane w ramach Straży Granicznej mające na celu zapewnienie zgodności wykorzystania danych SIS i danych VIS z obowiązującymi przepisami, przeprowadzono czynności kontrolne w Komendzie Głównej Straży Granicznej.

4. W wyniku kontroli przeprowadzonej w Komendzie Głównej Straży Granicznej (KGSG) stwierdzono, że kontrola działań użytkowników w Straży Granicznej mająca na celu zapewnienie zgodności wykorzystywania danych z obowiązującymi przepisami, o której

mowa w art. 24 ustawy o udziale Rzeczypospolitej Polskiej w Systemie Informacji Schengen oraz Wizowym Systemie Informacyjnym, jest sprawowana w przypadku, gdy dostęp do danych VIS realizowany jest poprzez system „ZSE6”. Natomiast ww. kontrola nie była realizowana w sytuacji, gdy dostęp do danych VIS następował przy wykorzystaniu aplikacji WWW VIS. Wobec powyższego Generalny Inspektor Ochrony Danych Osobowych zwrócił się do Komendanta Głównego Straży Granicznej o złożenie wyjaśnień w zakresie ww. nieprawidłowości.

5. W toku kontroli pozostałych organów posiadających dostęp do Wizowego Systemu Informacyjnego nie stwierdzono uchybień w procesie przetwarzania danych osobowych w zakresie objętym kontrolą.