BIURO
GENERALNEGO INSPEKTORA
OCHRONY DANYCH OSOBOWYCH

DIS-K-421/36/15

Protokół kontroli

W dniach 16 – 20 marca 2015 r., na podstawie art. 14 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2014 r. poz. 1182 z późn. zm.), w celu kontroli zgodności przetwarzania danych z przepisami o ochronie danych osobowych, dokonano czynności kontrolnych w Ministerstwie Sprawiedliwości z siedzibą w Warszawie przy Al. Ujazdowskich 11.

Z upoważnienia Generalnego Inspektora Ochrony Danych Osobowych czynności kontrolnych dokonali:

1. Krzysztof Staniak – inspektor
   legitymacja służbowa nr 331; upoważnienie nr 422/78/15
2. Rafał Grodzki – starszy inspektor
   legitymacja służbowa nr 332; upoważnienie nr 422/79/15

Wykaz aktów prawnych dotyczących kontroli:

1. Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2014 r. poz. 1182 z późn. zm.), zwana dalej ustawą.
2. Rozporządzenie 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. Przedmiot i zakres kontroli:

Kontrolą objęto przetwarzanie danych osobowych przez Ministra Sprawiedliwości, w związku z funkcjonowaniem systemu informatycznego SIS2 SAD, w następującym zakresie:

1. Czy Minister Sprawiedliwości posiada dostęp do danych SIS, a jeżeli tak to na jakiej podstawie prawnej, w jakim zakresie i celu, w szczególności za pośrednictwem systemu SIS2 SAD.
2. Czy prowadzone jest monitorowanie i rejestrowanie operacji wykonywanych przez użytkowników systemu SIS2 SAD na danych SIS, a także przez inne osoby.
3. Czy podmioty zewnętrzne posiadają dostęp do systemów informatycznych, poprzez które realizowany jest dostęp do danych SIS, w celu zapewnienia jego prawidłowego funkcjonowania, w tym na podstawie umów powierzenia przetwarzania danych (art. 31 ustawy).
4. Czy zostały zastosowane środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, w tym zabezpieczające dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem (art. 36 ust. 1 ustawy).
5. Czy prowadzona jest dokumentacja opisująca sposób przetwarzania danych oraz środki, o których mowa w art. 36 ust. 1 ustawy (art. 36 ust. 2 ustawy).
6. Czy powołany został administrator bezpieczeństwa informacji (art. 36a ust. 1 ustawy).
7. Czy osobom dopuszczonym do przetwarzania danych osobowych zostały nadane stosowne upoważnienia w tym zakresie (art. 37 ustawy).
8. Sposobu, w jaki zapewniana jest kontrola nad tym, jakie dane osobowe, kiedy i przez kogo zostały do zbioru wprowadzone oraz komu są przekazywane (art. 38 ustawy).
9. Czy prowadzona jest ewidencja osób upoważnionych do przetwarzania danych osobowych (art. 39 ustawy).
10. Kontrola systemu informatycznego w zakresie spełnienia wymogów określonych przepisami rozporządzenia 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).

II. Opis stanu faktycznego stwierdzonego w toku kontroli:

II. 1. Ustalenia ogólne

Minister Sprawiedliwości administruje systemem informatycznym o nazwie SIS2 SAD. Jednostką organizacyjną Ministerstwa odpowiedzialną za nadzór nad ww. systemem jest Departament Informatyzacji i Rejestrów Sądowych. Zakres zadań i tryb pracy komórek organizacyjnych Ministerstwa Sprawiedliwości został określony w Regulaminie Organizacyjnym Ministerstwa Sprawiedliwości wprowadzonym Zarządzeniem nr 59/15/BOF Ministra Sprawiedliwości z dnia 30 stycznia 2015 r. (kopia ww. regulaminu wraz z zarządzeniem stanowi załącznik nr 1). Struktura

organizacyjna Departamentu Informatyzacji i Rejestrów Sądowych została określona w Wewnętrznym regulaminie organizacyjnym Departamentu Informatyzacji i Rejestrów Sądowych (kopia ww. regulaminu stanowi załącznik nr 2). Obecnie Ministrem Sprawiedliwości jest Pan Cezary Grabarczyk. Minister Sprawiedliwości upoważnił w dniu 16 marca 2015 r. Panią Elizę Wójcik, Dyrektora Generalnego Ministerstwa Sprawiedliwości, do wykonywania w jego imieniu czynności związanych z kontrolą (kopia upoważnienia stanowi załącznik nr 3). Za pośrednictwem systemu SIS2 SAD Ministerstwo posiada dostęp do danych SIS wprowadzanych przez poszczególne sądy okręgowe i sądy apelacyjne.

II. 2. Ustalenia szczegółowe.

Jak ustalono, funkcjonowanie Systemu Informacyjnego Schengen w Ministerstwie Sprawiedliwości jest związane z realizacją dyspozycji wynikającej z ustawy z dnia 27 lipca 2001 r. Prawo o ustroju sądów powszechnych (Dz. U. z 2015 r., poz. 133), zgodnie z którą nadzór administracyjny nad działalnością sądów, o której mowa w art. 8 pkt 1, sprawuje Minister Sprawiedliwości (art. 9 tej ustawy). Zgodnie z art. 8 pkt 1 ww. ustawy działalność administracyjna sądów polega na zapewnieniu odpowiednich warunków techniczno-organizacyjnych oraz majątkowych funkcjonowania sądu i wykonywania przez sąd zadań, o których mowa w art. 1 § 2 i § 3. Pozycję Ministra Sprawiedliwości określa w szczególności art. 24 ust. 3 ustawy z dnia 4 września 1997 r. o działach administracji rządowej (Dz. U. z 2013 r., poz. 743 z późn. zm.). Zgodnie z tym przepisem, Minister Sprawiedliwości jest właściwy do spraw sądownictwa w zakresie niezastrzeżonym odrębnymi przepisami do kompetencji innych organów państwowych i z uwzględnieniem zasady niezawisłości sędziowskiej. W związku ze wskazanymi potrzebami Minister Sprawiedliwości wykonuje m.in. następujące zadania: prowadzenie spraw związanych z informatyzacją resortu sprawiedliwości, prowadzenie spraw związanych z eksploatacją systemów informatycznych resortu sprawiedliwości, zapewnienie prawidłowego funkcjonowania i obsługi systemów, urządzeń i rozwiązań informatycznych wykorzystywanych w resorcie sprawiedliwości, w tym sprawowania nadzoru nad ich obsługą i eksploatacją. Wykonuje również zadania związane z zapewnieniem bezpieczeństwa systemów informatycznych i baz danych, w szczególności ich ochrony przed nieuprawnionym dostępem, zniszczeniem oraz utratą danych. Prawidłowe funkcjonowanie w sądach Systemu Informacyjnego Schengen (SIS2 SAD) wymaga zaangażowania Ministerstwa Sprawiedliwości, które zapewnia jego utrzymanie dla potrzeb sądów powszechnych. Jednocześnie Minister Sprawiedliwości nie wykorzystuje danych zawartych w systemie do wykonywania jakichkolwiek czynności mających skutki prawne dla jego funkcjonowania. Jego rola ogranicza się jedynie do zapewnienia dostępu dla sądów do ww. systemu w zakresie przewidzianym w przepisami ustawy z dnia 24 sierpnia 2007 r. o udziale Rzeczpospolitej Polskiej w Systemie Informacyjnym

Schengen oraz Wizowym Systemie Informacyjnym (t.j. Dz. U. z 2014 r., poz. 1203) – pismo z dnia 27 marca 2015 r. Dyrektora Generalnego Ministerstwa Sprawiedliwości BKA-VII-0910-1/15 stanowi załącznik nr 4.

Jak wyjaśnił Pan [redacted] starszy specjalista (protokół przyjęcia ustnych wyjaśnień stanowi załącznik nr 5) w Ministerstwie dostęp do danych SIS przetwarzanych w ramach systemu SIS2 SAD posiada pięć osób. Ww. osoby otrzymały upoważnienie do przetwarzania danych osobowych w zbiorze danych SIS2 SAD (kopie upoważnień do przetwarzania danych stanowią załącznik nr 6). Zastępca Dyrektora Departamentu Informatyzacji i Rejestrów Sądowych nie posiada dostępu do danych SIS przetwarzanych w ww. systemie (kopia upoważnienia stanowi załącznik nr 7). Osoby te nie posiadają żadnych upoważnień nadanych przez Centralny Organ Techniczny KSI Komendy Głównej Policji, nie były także szkolone z zakresu bezpieczeństwa i ochrony danych osobowych wykorzystywanych poprzez KSI, za wyjątkiem Pana [redacted] Pan [redacted] otrzymał zaświadczenie dla trenerów z zakresu prawnych i technicznych aspektów użytkownika Systemu Informacyjnego Schengen drugiej generacji (SISII) – kopia ww. zaświadczenia stanowi załącznik nr 8). Administratorem systemu informatycznego o nazwie „SIS2 SAD" jest Pan [redacted] pełnił on również do dnia 18 marca 2015 r. funkcję administratora bezpieczeństwa informacji w Departamencie Informatyzacji i Rejestrów Sądowych (protokół przyjęcia ustnych wyjaśnień od Pana [redacted] stanowi załącznik nr 9).

Minister Sprawiedliwości posiada pełen wgląd do danych SIS, może dokonywać zmiany lub usunięcia danych SIS, jednak takich czynności nie realizuje z uwagi na to, iż uprawnienia takie posiadają wyłącznie sądy. Ministerstwo posiada wgląd we wszystkie wpisy danych SIS dokonane przez sądy. Dotychczas sądy apelacyjne nie dokonywały wpisów ani wglądu do danych SIS, wszystkie konta użytkowników końcowych z sądów apelacyjnych zostały zablokowane.

W Ministerstwie opracowano ewidencję osób upoważnionych do przetwarzania danych w systemami informatycznym o nazwie SIS2 SAD (kopia ewidencji stanowi załącznik nr 10). Użytkownicy końcowi posiadający dostęp do danych SIS w sądach apelacyjnych i okręgowych otrzymali upoważnienia do dostępu do Krajowego Systemu Informatycznego oraz wykorzystania danych SIS w celu wglądu i wpisu danych SIS (kopie przykładowych upoważnień stanowią załącznik nr 11). W Ministerstwie prowadzony jest „Wykaz użytkowników SIS2 SAD" (wydruk ww. wykazu stanowi załącznik nr 12). Ww. użytkownicy są szkoleni cyklicznie raz do roku, osoby na szkolenia są zgłaszane przez prezesów poszczególnych sądów (kopia przykładowej dokumentacji dotyczącej przeprowadzonych szkoleń stanowi załącznik nr 13). Po zakończonych szkoleniach ww. osoby otrzymują zaświadczenia o ukończeniu szkolenia (kopie przykładowych zaświadczeń stanowią załącznik nr 14).

Procedura nadawania uprawnień nowemu użytkownikowi została opisana w dokumencie o nazwie „Instrukcja nadawania uprawnień do systemu SIS2 SAD", która stanowi załącznik do „Polityki bezpieczeństwa systemu SIS2 SAD", instrukcja ta określa także sposób odbierania uprawnień do ww. systemu (przykładowa dokumentacja dotycząca nadawania uprawnień w systemie SIS2 SAD stanowi załącznik nr 15, przykładowa dokumentacja dotycząca odbierania uprawnień do systemu SIS2 SAD stanowi załącznik nr 16). Blokowanie konta użytkownika końcowego w systemie SIS2 SAD następuje w terminie 30 – 40 dni i jest realizowane przez administratora systemu w Ministerstwie.

Ponadto, Minister Sprawiedliwości zawarł umowę nr 6 z dnia 27 lutego 2015 r. z Sygnity S.A. z siedzibą w Warszawie przy al. Jerozolimskie 180 dotyczącą prowadzenia nadzoru nad eksploatacją, świadczenie serwisu i wsparcia technicznego dla systemu SIS2 SAD, modyfikacji tego systemu (kopia ww. umowy wraz z załącznikami stanowi załącznik nr 17). Ww. podmiot będzie miał dostęp do danych SIS za pośrednictwem systemu SIS2 SAD. Osobom z tego podmiotu zostaną nadane upoważnienia do przetwarzania danych osobowych w tym systemie, w zakresie wglądu do danych. Poprzednie upoważnienia dla przedstawicieli ww. podmiotu utraciły ważność (kopie tych upoważnień stanowią załącznik nr 18).

W Ministerstwie prowadzone jest rejestrowanie operacji wykonywanych przez użytkowników końcowych systemu SIS2 SAD na danych SIS. System SIS2 SAD nie posiada funkcjonalności umożliwiającej wygenerowanie raportu zawierającego informacje o ruchu/aktywności użytkownika końcowego w tym systemie. Dotychczas żaden z sądów nie zwracał się do Ministerstwa o udzielenie informacji dotyczącej ruchu użytkowników końcowych w systemie SIS2 SAD.

W Ministerstwie pięć osób ([redacted] posiada dostęp do logów systemowych ww. systemu, natomiast dwóch pracowników (tj. [redacted] posiada dostęp do aplikacji i bazy danych systemu SIS2 SAD. W Ministerstwie nie jest prowadzona rejestracja operacji wykonywanych przez administratorów systemu SIS2 SAD. Dostęp do danych systemu SIS2 SAD realizowany jest w Ministerstwie przez ww. osoby za pośrednictwem aplikacji DB2 IBM Studio, jest to aplikacja zarządzająca bezpośrednio bazą danych ww. systemu. Aplikacja ta umożliwia dostęp do wszystkich danych SIS z sądów, na których można dokonać następujących operacji m.in. „sprawdzenie", „usunięcie", „modyfikacja", „utworzenie", „przeglądanie". Obecnie administratorzy dokonują wglądu do danych SIS, w sytuacji gdy użytkownik zgłosi problem techniczny dotyczący konkretnej operacji na wpisie. Zgłoszenie problemu odbywa się telefonicznie lub e-mailem. W takiej sytuacji dokonywana jest weryfikacja użytkownika końcowego oraz analiza zgłoszonego problemu.

W toku czynności kontrolnych ustalono, że w dniu 19 marca 2015 roku został przesłany do Ministerstwa dokument o nazwie „Polityka Bezpieczeństwa KSI Centralnego Organu Technicznego dla Organów i Służb wersja 1.3.1 z lipca 2014 r." (wydruk treści emaila, do którego załączono ww.

dokumentu stanowi załącznik nr 19, wydruk Polityki Bezpieczeństwa KSI Centralnego Organu Technicznego dla Organów i Służb wersja 1.3.1 z lipca 2014 r. stanowi załącznik nr 20).

Zgodnie z pismem Pana Jerzego Sipa, Dyrektora Biura Łączności i Informatyki KGP z dnia 14 lutego 2013 r. wyznaczono Pana [redacted] na funkcję Inspektora Rejestracji (IR) w zakresie wydania certyfikatów uwierzytelniających dla serwerów i innych urządzeń wykorzystywanych przez system teleinformatyczny Ministerstwa Sprawiedliwości SIS2 SAD umożliwiający dostęp do KSI w obszarze funkcjonowania Systemu Informacyjnego Schengen drugiej generacji (SIS II) (kopia ww. pisma wraz z kopiami wniosków o wydanie certyfikatu Klucza Publicznego dla użytkownika instytucjonalnego z 2014 roku stanowi załącznik nr 21).

Decyzją nr RU/MS/30/2015 Ministra Sprawiedliwości z dnia 18 marca 2015 r. powołano Pana [redacted] – radcę ministra w Biurze Kontroli i Audytu Wewnętrznego do pełnienia roli Administratora Bezpieczeństwa Informacji w Ministerstwie Sprawiedliwości (kopia decyzji nr RU/MS/30/2015 Ministra Sprawiedliwości z dnia 18 marca 2015 r. stanowi załącznik nr 22, kopia Decyzji nr RU/DG/24/2015 Dyrektora Generalnego Ministerstwa Sprawiedliwości z dnia 17 marca 2015 r. stanowi załącznik nr 23, kopia decyzji Nr BO-113-162/13/1 Dyrektora Generalnego Ministerstwa Sprawiedliwości z dnia 11 kwietnia 2013 r. stanowi załącznik nr 24, kopia Decyzji Nr BO-113-568/13 Ministra Sprawiedliwości z dnia 19 grudnia 2013 r. stanowi załącznik nr 25, kopia Decyzji Nr 3/12/BINiSO Ministra Sprawiedliwości z dnia 3 października 2012 r. stanowi załącznik nr 26, kopia Decyzji Nr 1/12/BINiSO Ministra Sprawiedliwości z dnia 3 października 2012 r. stanowi załącznik nr 27).

Jak wyjaśnił Pan [redacted] (protokół przyjęcia ustnych wyjaśnień stanowi załącznik nr 28), w Ministerstwie Sprawiedliwości zostały wdrożone następujące dokumenty opisujące proces przetwarzania danych osobowych tj.: „Polityka bezpieczeństwa Informacji Ministerstwa Sprawiedliwości wersja 1.0" (kopia ww. dokumentu stanowi załącznik nr 29), „Polityka bezpieczeństwa systemów teleinformatycznych Ministerstwa Sprawiedliwości wersja 1.0" (kopia ww. dokumentu stanowi załącznik nr 30), „Regulamin Użytkowania Systemów Teleinformatycznych Ministerstwa Sprawiedliwości wersja 1.0" (kopia ww. dokumentu stanowi załącznik nr 31), „Polityka Bezpieczeństwa Systemu Informatycznego SIS2 SAD wersja 1.0 (kopia ww. dokumentu stanowi załącznik nr 33). Powyższe dokumenty zostały wdrożone Zarządzeniem Ministra Sprawiedliwości z dnia 27 czerwca 2012 r. w sprawie wprowadzenia Polityki Bezpieczeństwa Informacji Ministerstwa Sprawiedliwości i sądów powszechnych (kopia Zarządzenia Ministra Sprawiedliwości z dnia 27 czerwca 2012 r. wraz z załączoną Polityką Bezpieczeństwa Informacji Ministerstwa Sprawiedliwości i sądów powszechnych stanowi załącznik nr 32).

W Ministerstwie Sprawiedliwości opracowana „Politykę Bezpieczeństwa Systemu Informatycznego SIS2 SAD wersja 2.0 (kopia ww. dokumentu wraz z załącznikami oraz wskazanymi w niej odnośnikami stanowi załącznik nr 34). Jak wyjaśnił Pan [redacted] (protokół przyjęcia

ustnych wyjaśnień stanowi załącznik nr 28), Polityka Bezpieczeństwa Systemu Informatycznego SIS2 SAD wersja 2.0 nie została wdrożona przez administratora danych.

Jak wyjaśnił Pan [redacted] (protokół przyjęcia ustnych wyjaśnień stanowi załącznik nr 35), Ministerstwo Sprawiedliwości nie przekazywało dotychczas do sądów dokumentacji opisującej sposób przetwarzania danych osobowych w systemie „SIS2 SAD", w szczególności informacji wskazanych w § 4 pkt 1, pkt 3, pkt 4, pkt 5 rozporządzenia 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), dotyczących systemu informatycznego o nazwie „SIS2 SAD".

Oględziny serwerowni

W toku czynności kontrolnych ustalono, że serwerownia znajduje się na parterze w budynku Ministerstwa Sprawiedliwości przy ul. Czerniakowskiej 100 w Warszawie (protokół oględzin serwerowni stanowi załącznik nr 36). Pomieszczenia serwerowni oraz korytarze wejściowe stanowią strefę bezpieczeństwa, do której dostęp posiadają tylko osoby upoważnione. Dostęp do ww. strefy realizowany jest z wykorzystaniem czytników kart zbliżeniowych. Wejście do strefy, z której możliwy jest dostęp do serwerowni realizowane jest poprzez video domofon. Pracownik musi zweryfikować konieczność wejścia i zezwolić na wejście osób trzecich. Osoby trzecie mogą przebywać i wykonywać czynności tylko w pod nadzorem. Dojście do drzwi wejściowych strefy bezpieczeństwa oraz cała strefa bezpieczeństwa jest monitowana przez system kamer przemysłowych. Obraz z kamer jest przesyłany do centrali całodobowego posterunku służb ochrony budynku. Wejście do serwerowni zabezpieczone jest systemem kontroli dostępu (czytnik kart zbliżeniowych).

Pomieszczenie serwerowni nie posiada okien jest klimatyzowane, i wyposażone w czujki temperatury, czujki ruchu i czujki ppoż. Serwery ustawione są na podniesionej podłodze technicznej. Przed zanikiem napięcia i awarią zasilania serwery oraz urządzenia sieci teleinformatycznej zabezpieczone są poprzez UPS. Serwerownia zabezpieczona jest system gaszenia gazem FM-200. Serwer, na którym postawiony jest system SIS2 SAD znajduje się w szafie typu Rack. System składa się z aplikacji SIS2 SAD oraz bazy danych IBM DB2. Aplikacja oraz baza danych są zainstalowane na systemach operacyjnych Microsoft Windows Server 2008 R2 Enterprise. System jest zabezpieczony programem antywirusowym. Aktualizacja oprogramowania antywirusowego jest na bieżąco aktualizowana o nowe sygnatury. Dostęp do ww. serwera zabezpieczony jest mechanizmem logowania administratora. Hasło administratora składają się co najmniej z 8 znaków i zawierają, małe wielkie litery oraz cyfry i znaki specjalne.

Sieć teleinformatyczna

Jak wyjaśnił Pan [redacted] (protokół przyjęcia ustnych wyjaśnień stanowi załącznik nr 37), Ministerstwo Sprawiedliwości połączenie jest z KGP COT KSI siecią teleinformatyczna KGP MEWA. W budynku Ministerstwa Sprawiedliwości mieszczącym się przy ulicy Czerniakowskiej 100 w Warszawie, w pomieszczeniu 123 (Punkcie Dystrybucyjnym PD1) jest doprowadzone dedykowane łącze światłowodowe Komendy Głównej Policji realizujące połączenie z siecią MEWA. W ramach tego połączenia funkcjonuje dostęp do Systemu Informacyjnego Schengen (SIS II). Role urządzenia bezpieczeństwa po stronie Ministerstwa Sprawiedliwości spełnia dedykowane urządzenie Firewall Cisco ASA 5510, terminujące bezpieczne szyfrowanego połączenia VPN (IPSEC VPN). Urządzenie posiada wgrany certyfikat wystawiony przez Operacyjny Urząd Certyfikacji – Centrum Certyfikacji KSI. Certyfikat ten posiada roczną datę ważności natomiast jego odnowienie jest wykonywane zgodnie z polityką certyfikacji KSI. Serwery realizujące dostęp do systemu SIS II dla resortu sprawiedliwości są w odseparowanej sieci VLAN. Sieć ta nie ma styku z siecią publiczną (Internet). Dostęp po stronie sądów jest realizowany z wykorzystaniem sieci WAN resortu sprawiedliwości odseparowanej od sieci Internet. Sieć WAN MS jest w standardzie MPLS VPN, działa w oparciu o wydzielony(dedykowany) szkielet IP MPLS przeznaczony tylko do przenoszenia ruchu klientów VPN. Struktura logiczna sieci jest kreowana w ramach fizycznej infrastruktury sieci rozległej Wykonawcy, w sposób zapewniający możliwości zestawiania połączeń pomiędzy użytkownikami sieci transmisji danych w warstwie trzeciej modelu OSI (ang. Virtual PrivateNetwork). Ruch w sieci Operatora odseparowany jest od pozostałych klientów za pomocą wirtualnych tablic routingu.

System informatyczny SIS2 SAD

W toku czynności kontrolnych ustalono, że w pomieszczeniu nr 219 w budynku Ministerstwa Sprawiedliwości w Warszawie przy ul. Czerniakowskiej 100 w Warszawie w Departamencie Informatyzacji i Rejestrów Sądowych możliwy jest dostęp do danych przetwarzanych w bazie danych SIS II. Dostęp taki jest realizowany za pośrednictwem systemu SIS2 SAD. Kontrolowana stacja komputerowa, przy pomocy której możliwy był dostęp do systemu SIS2 SAD pracuje przy pomocy systemu operacyjnego Windows 7 Pro. Stacja komputerowa wykorzystywana jest wyłącznie do dostępu do systemu SIS2 SAD (protokół oględzin stanowi załącznik nr 38). Dostęp do systemu operacyjnego ww. stacji komputerowej zabezpieczony jest mechanizmem uwierzytelnienia użytkownika i wymaga wprowadzenia identyfikatora oraz hasła. Hasło do systemu operacyjnego Pana [redacted] składało się z co najmniej 8 znaków i zawierało małe, wielkie litery oraz cyfry. Ustalono, że hasło do systemu operacyjnego zmieniane jest przez wymuszenie systemowe co 30 dni. Stacja komputerowa nie posiadała dostępu do sieci internet i pracuje w sieci Ministerstwa

Sprawiedliwości. Dodatkowo stacja ta posiadała system antywirusowy. System antywirusowy w dniu 19 marca 2015 roku posiadał definicję wirusów z dnia 19 marca 2015.r.

W celu uruchomienia systemu SIS2 SAD (system webowy) należy uruchomić przeglądarkę internetową Internet Explorer oraz wprowadzić odpowiedni numer IP serwera. Po uruchomieniu przeglądarki i wprowadzeniu adresu IP systemu webowego, otwiera okno przeglądarki internetowej z opcją logowania do systemu (wydruk zrzutu ekranu z oknem logowania do systemu SIS2 SAD stanowi załącznik nr 39). W celu zalogowania do systemu SIS2 SAD należy podać nazwę użytkownika oraz hasło. Hasło Pana [redacted] (administratora systemu) składa się z co najmniej 8 znaków i zawiera, małe, wielki litery oraz cyfry. Hasło to jest zmieniane co 30 dni poprzez wymuszenie systemowe. Po zalogowaniu do systemu uzyskano dostęp do menu systemu (wydruk zrzutów ekranu z menu głównym systemu SIS2 SAD stanowi załącznik nr 40). W systemie SIS2 SAD administrator ma dostęp do następujących kategorii: Folder SIS I (archiwum), Folder SIS II. W folderze SIS II dostępne są następujące podkategorie: „Wyszukanie właściciela wpisu", „Przeglądanie zadań", „Przedłużenie daty ważności wpisu", „"Dostosowanie wpisu", „Osoba", „Pojazd", „Dowód rejestracyjny pojazdu", „Tablice rejestracyjne", „Dokument wydany", „Banknot", „Łódź", „Silnik Łodzi", „Samolot", „Broń palna", „Blankiet dokumentu", „Urządzenia przemysłowe", „Papiery Wartościowe", „Kontener".

Po rozwinięciu podkategorii „Osoba" możliwe jest m.in. dokonanie sprawdzenia osoby, bądź dokonania wpisu. W celu dokonania sprawdzenia osoby uruchamiana jest podkategoria „Sprawdzenie". W celu dokonania sprawdzenia należy wpisać następujące dane: nazwisko, imiona, data urodzenia, płeć, obywatelstwo (wydruk zrzutu ekranu z oknem sprawdzenia osoby stanowi załącznik nr 41). W celu dokonania wpisu osoby należy uruchomić podkategorię o nazwie „Nowy obiekt". W celu dokonania wpisu nowej osoby należy wprowadzić dane na formularzu, który składa się z 6 kroków (zrzuty ekranu z pierwszym krokiem wprowadzania wpisu dotyczącego danej osoby stanowią załącznik nr 42).

Po rozwinięciu podkategorii „Pojazd" możliwe jest m.in. dokonanie sprawdzenia pojazdu, bądź dokonania wpisu. W celu dokonania sprawdzenia pojazdu uruchamiana jest podkategoria „Sprawdzenie". W celu dokonania sprawdzenia należy wpisać następujące dane: marka, kolor, typ, kraj rejestracji, numer rejestracyjny, numer VIN, identyfikator zestawu, numer etykiety (wydruk zrzutu ekranu z oknem przeglądania wpisów pojazdu stanowi załącznik nr 43). W celu dokonania wpisu pojazdu należy uruchomić podkategorię o nazwie „Nowy obiekt". W celu dokonania wpisu pojazdu należy wprowadzić dane na formularzu, który składa się z 3 kroków (zrzuty ekranu z 1 krokiem wprowadzania wpisu dotyczącego pojazdu stanowią załącznik nr 44).

Po rozwinięciu podkategorii „Dowód rejestracyjny pojazdu" możliwe jest m.in. dokonanie sprawdzenia dowodu rejestracyjnego pojazdu, bądź dokonania wpisu. W celu dokonania sprawdzenia

dowodu rejestracyjnego pojazdu uruchamiana jest podkategoria „Sprawdzenie" (wydruk zrzutu ekranu z oknem przeglądania wpisów dowód rejestracyjny pojazdu stanowi załącznik nr 45). W celu dokonania sprawdzenia należy wpisać następujące dane: kraj wydania dokumentu, numer rejestracyjny. W celu dokonania wpisu dowodu rejestracyjnego pojazdu należy uruchomić podkategorię o nazwie „Nowy obiekt". W celu dokonania wpisu dowodu rejestracyjnego pojazdu należy wprowadzić dane na formularzu, który składa się z 2 kroków (zrzuty ekranu z 1 krokiem wprowadzania wpisu dotyczącego dowodu rejestracyjnego pojazdu stanowią załącznik nr 46).

Po rozwinięciu podkategorii „Tablice rejestracyjne" możliwe jest m.in. dokonanie sprawdzenia tablic rejestracyjnych, bądź dokonania wpisu tablic rejestracyjnych. W celu dokonania sprawdzenia tablic rejestracyjnych uruchamiana jest podkategoria „Sprawdzenie". W celu dokonania sprawdzenia należy wpisać następujące dane: kraj rejestracji, numer rejestracji (wydruk zrzutu ekranu z oknem przeglądania wpisów tablic rejestracyjnych stanowi załącznik nr 47). W celu dokonania wpisu tablic rejestracyjnych należy uruchomić podkategorię o nazwie „Nowy obiekt". W celu dokonania wpisu tablic rejestracyjnych należy wprowadzić dane na formularzu, który składa się z 2 kroków (zrzuty ekranu z 1 krokiem wprowadzania wpisu dotyczącego tablic rejestracyjnych stanowią załącznik nr 48).

Po rozwinięciu podkategorii „dokument wydany" możliwe jest m.in. dokonanie sprawdzenia wydanego dokumentu, bądź dokonania wpisu. W celu dokonania sprawdzenia kategorii dokument wydany uruchamiana jest podkategoria „Sprawdzenie". W celu dokonania sprawdzenia należy wpisać następujące dane: kategoria, państwo, data urodzenia, nazwisko, imię, numer 1 dokumentu, numer 2 dokumentu (wydruk zrzutu ekranu z oknem przeglądania wpisów wydanego dokumentu stanowi załącznik nr 49). W celu dokonania wpisu wydanego dokumentu należy uruchomić podkategorię o nazwie „Nowy obiekt". W celu dokonania wpisu wydanego dokumentu należy wprowadzić dane na formularzu, który składa się z 2 kroków (zrzuty ekranu z 1 krokiem wprowadzania wpisu dotyczącego dokument wydany stanowią załącznik nr 50).

Po rozwinięciu podkategorii „Banknot" możliwe jest m.in. dokonanie sprawdzenia banknotu, bądź dokonania jego wpisu. W celu dokonania sprawdzenia kategorii banknot uruchamiana jest podkategoria „Sprawdzenie". W celu dokonania sprawdzenia należy wpisać następujące dane: waluta, numer 1, numer 2, wartość, identyfikator użytkownika (wydruk zrzutu ekranu z oknem przeglądania wpisów banknotu stanowi załącznik nr 51). W celu dokonania wpisu wydanego dokumentu należy uruchomić podkategorię o nazwie „Nowy obiekt". W celu dokonania wpisu banknotu należy wprowadzić dane na formularzu, który składa się z 2 kroków (zrzut ekranu z 1 krokiem wprowadzania wpisu dotyczącego banknotu stanowią załącznik nr 52).

Po rozwinięciu podkategorii „Łódź" możliwe jest m.in. dokonanie sprawdzenia łodzi, bądź dokonania wpisu łodzi. W celu dokonania sprawdzenia kategorii łódź uruchamiana jest podkategoria „Sprawdzenie". W celu dokonania sprawdzenia należy wpisać następujące dane: kraj rejestracji, kolor

numer na żaglu, numer seryjny, identyfikator zewnętrzny, numer rejestracyjny, numer certyfikatu, numer identyfikacyjny kadłuba, nazwa łodzi (wydruk zrzutu ekranu z oknem przeglądania wpisów łodzi stanowi załącznik nr 53). W celu dokonania wpisu łodzi należy uruchomić podkategorię o nazwie „Nowy obiekt". W celu dokonania wpisu danej łodzi należy wprowadzić dane na formularzu, który składa się z 2 kroków (zrzut ekranu z 1 krokiem wprowadzania wpisu dotyczącego łodzi stanowią załącznik nr 54).

Po rozwinięciu podkategorii „silnik łódź" możliwe jest m.in. dokonanie sprawdzenia silnika łodzi, bądź dokonania wpisu silnika łodzi. W celu dokonania sprawdzenia kategorii silnik łódzi uruchamiana jest podkategoria „Sprawdzenie". W celu dokonania sprawdzenia należy wpisać następujące dane: kategoria, marka/producent, numer seryjny (wydruk zrzutu ekranu z oknem przeglądania wpisów silnika łodzi stanowi załącznik nr 55). W celu dokonania wpisu silnika łodzi należy uruchomić podkategorię o nazwie „Nowy obiekt". W celu dokonania wpisu silnika łodzi należy wprowadzić dane na formularzu, który składa się z 2 kroków (zrzut ekranu z 1 krokiem wprowadzania wpisu dotyczącego silnik łodzi stanowią załącznik nr 56).

Po rozwinięciu podkategorii „samolot" możliwe jest m.in. dokonanie sprawdzenia samolotu, bądź dokonania wpisu samolotu. W celu dokonania sprawdzenia kategorii samolot uruchamiana jest podkategoria „Sprawdzenie". W celu dokonania sprawdzenia należy wpisać następujące dane: kolor, numer seryjny, indywidualna nazwa samolotu, identyfikator ICAO (wydruk zrzutu ekranu z oknem przeglądania wpisów samolotu stanowi załącznik nr 57). W celu dokonania wpisu samolotu należy uruchomić podkategorię o nazwie „Nowy obiekt". W celu dokonania wpisu należy wprowadzić dane na formularzu, który składa się z 2 kroków (zrzut ekranu z 1 krokiem wprowadzania wpisu dotyczącego samolotu stanowią załącznik nr 58).

Po rozwinięciu podkategorii „broń palna" możliwe jest m.in. dokonanie sprawdzenia, bądź dokonania wpisu. W celu dokonania sprawdzenia uruchamiana jest podkategoria o nazwie „Sprawdzenie". W celu dokonania sprawdzenia broni palnej należy wpisać następujące dane: marka/producent, kategoria, kaliber, numer broni, model. W celu dokonania wpisu broni palnej należy uruchomić podkategorię o nazwie „Nowy obiekt". W celu dokonania wpisu należy wprowadzić dane na formularzu, który składa się z 2 kroków (zrzut ekranu z 1 krokiem wprowadzania wpisu dotyczącego broni palnej stanowią załącznik nr 59).

Po rozwinięciu podkategorii „blankiet dokumentu" możliwe jest m.in. dokonanie sprawdzenia, bądź dokonania wpisu. W celu dokonania sprawdzenia uruchamiana jest podkategoria o nazwie „Sprawdzenie". W celu dokonania sprawdzenia należy wpisać następujące dane: kategoria dokumentu, państwo, numer dokumentu (wydruk zrzutu ekranu z oknem przeglądania wpisów blankietu dokumentu stanowi załącznik nr 60). W celu dokonania wpisu blankietu dokumentu należy uruchomić podkategorię o nazwie „Nowy obiekt". W celu dokonania wpisu należy wprowadzić dane na

formularzu, który składa się z 2 kroków (zrzut ekranu z 1 krokiem wprowadzania wpisu dotyczącego blankietu dokumnetów stanowią załącznik nr 61).

Po rozwinięciu podkategorii „urządzenie przemysłowe" możliwe jest m.in. dokonanie sprawdzenia, bądź dokonania wpisu. W celu dokonania sprawdzenia uruchamiana jest podkategoria o nazwie „Sprawdzenie". W celu dokonania sprawdzenia należy wpisać następujące dane: kategoria, marka/producent, typ, numer silnika, numer seryjny, numer VIN, numer rejestracyjny (wydruk zrzutu ekranu z oknem przeglądania wpisów urządzenia przemysłowego stanowi załącznik nr 62). W celu dokonania wpisu urządzenia przemysłowego należy uruchomić podkategorię o nazwie „Nowy obiekt". W celu dokonania wpisu należy wprowadzić dane na formularzu, który składa się z 2 kroków (zrzut ekranu z 1 krokiem wprowadzania wpisu dotyczącego urządzenia przemysłowego stanowią załącznik nr 63).

Po rozwinięciu podkategorii „Papiery wartościowe" możliwe jest m.in. dokonanie sprawdzenia, bądź dokonania wpisu. W celu dokonania sprawdzenia uruchamiana jest podkategoria o nazwie „Sprawdzenie". W celu dokonania sprawdzenia należy wpisać następujące dane: kategoria, waluta, wartość nominalna, numer ISIN (wydruk zrzutu ekranu z oknem przeglądania wpisu papierów wartościowych stanowi załącznik nr 64). W celu dokonania wpisu urządzenia przemysłowego należy uruchomić podkategorię o nazwie „Nowy obiekt". W celu dokonania wpisu należy wprowadzić dane na formularzu, który składa się z 2 kroków (zrzut ekranu z 1 krokiem wprowadzania wpisu dotyczącego papierów wartościowych stanowią załącznik nr 65).

Po rozwinięciu podkategorii „Kontener" możliwe jest m.in. dokonanie sprawdzenia, bądź dokonania wpisu. W celu dokonania sprawdzenia uruchamiana jest podkategoria o nazwie „Sprawdzenie". W celu dokonania sprawdzenia należy wpisać następujące dane: numer BIC (wydruk zrzutu ekranu z oknem przeglądania wpisu kontener stanowi załącznik nr 66). W celu dokonania wpisu kontenera należy uruchomić podkategorię o nazwie „Nowy obiekt". W celu dokonania wpisu należy wprowadzić dane na formularzu, który składa się z 2 kroków.

System informatyczny SIS2 SAD umożliwia sporządzenie i wydrukowanie informacji o odnotowaniach tj.: imienia i nazwiska użytkownika oraz jednostki organizacyjnej wykonującej operacje dokonania wpisu oraz daty i godziny dokonania wpisu. Z powyższych informacji generowany jest raport w formie pliku PDF (przykładowy wydruk potwierdzający powyższe funkcjonalności stanowi załącznik nr 67).

W systemie SIS2 SAD nie możliwe jest wyszukanie operacji dla danego użytkownika, możliwe jest jedynie wyszukanie operacji wykonanych przez dany sąd.

Systemie SIS2 SAD wyszukanie danych możliwe jest po zdefiniowanych operacjach takich m.in. jak: sprawdzenie, modyfikacja, usuniecie, zgłoszenie, rozszerzenie, przedłużenie ważności, pobieranie ENA (przykładowy wydruk z operacji rozszerzenie stanowi załącznik nr 68, przykładowy

wydruk z przedłużenia ważności stanowi załącznik nr 69, przykładowy wydruk z operacji usunięcia stanowi załącznik nr 70, przykładowy wydruk z operacji modyfikacji stanowi załącznik nr 71, przykładowy wydruk z operacji pobrania ENA stanowi załącznik nr 72, wydruk przykładowego Europejskiego Nakazu Aresztowania stanowi załącznik nr 73, przykładowy wydruk z odmową dokonania wpisu stanowi załącznik nr 74).

Ustalono, że system SIS2 SAD tworzy logi, które zapisywane są na dyskach serwera. Logi tworzone są w trybie dziennym oraz miesięcznym. Logi wykonywane są z wszystkich operacji użytkowników systemu SIS2 SAD. Logi zapisywane są w formacie XML. W logach zapisywana jest informacja o tym jaki sąd, kiedy oraz w jakim zakresie dokonał operacji. W logach część danych jest szyfrowana przez system SIS2 SAD, dane imię, nazwisko oraz Schengen ID nie są szyfrowane.

W toku kontroli ustalono, że w logach systemu SIS2 SAD zapisywana jest informacja w zakresie następujących czynności: złożenie zapytania w zakresie rozszerzenie, modyfikacja, sprawdzenie, usunięcie, zgłoszenie, przedłużenie ważności, sprawdzenie uzupełniające, usunięcie danych binarnych; w zakresie odpowiedzi: sprawdzenie, sprawdzenie uzupełniające, rozszerzenie, modyfikacja, usunięcie, zgłoszenie (wydruki z logów ze złożenia zapytania w zakresie rozszerzenie, modyfikacja, sprawdzenie, usunięcie, zgłoszenie, przedłużenie ważności, sprawdzenie uzupełniające, usunięcie danych binarnych stanowią załącznik nr 75, wydruki z logów odpowiedzi w zakresie sprawdzenie, sprawdzenie uzupełniające, rozszerzenie, modyfikacja, usunięcie, zgłoszenie stanowią załącznik nr 76).

Aplikacja zarządzająca bazą danych DB2 IBM Studio

W toku czynności kontrolnych ustalono, że administratorzy systemu SIS2 SAD posiadają dostęp do bazy danych ww. systemu za pośrednictwem aplikacji zarządzającej bazą danych DB2 IBM Studio (protokół oględzin stanowi załącznik nr 77).Ww. aplikacja umożliwia administratorom zarządzanie bazą danych w pełnym jego zakresie, w szczególności dotyczy: wglądu w dane, modyfikację danych, wprowadzanie danych.

Ustalono, że zarówno od strony aplikacji DB2 IBM Studia, jak i od strony bazy danych nie są tworzone logi, w których miałoby zostać zapisane wszelkie czynności wykonywane przez administratorów tj.: przeglądanie danych, wprowadzanie danych, modyfikację danych.

Dostęp do ww. aplikacji zabezpieczony jest procesem uwierzytelnienia użytkownika poprzez wprowadzenie identyfikatora oraz hasła. Hasło administratora do ww. aplikacji składa z co najmniej 8 znaków. Ponadto dostęp do ww. aplikacji zabezpieczony jest na poziomie systemu operacyjnego poprzez podanie indywidualnego loginu i hasła zgodnie z polityką bezpieczeństwa Ministerstwa Sprawiedliwości.

W toku kontroli ustalono, że w systemie SIS2 SAD nie jest rejestrowany (zapisywany do logu systemu) wgląd w dane przetwarzane w bazie danych systemu SIS2 SAD (w szczególności dotyczy to przeglądania konkretnych danych bez wykonywania sprawdzeń). W systemie SIS2 SAD rejestrowany jest fakt zalogowania się użytkownika systemu.

Dokonane poprawki, skreślenia, uzupełnienia:

.....

.....

.....

.....

Niniejszy protokół sporządzono w dwóch jednobrzmiących egzemplarzach.

Warszawa, dnia 16 kwietnia 2015 r.

Krysiak / Stanicki

.....

.....

(podpisy osób kontrolujących)

POUCZENIE:

Na podstawie art. 16 ust. 2 ustawy o ochronie danych osobowych, kontrolowanemu administratorowi danych przysługuje prawo złożenia umotywowanych zastrzeżeń i uwag.

Na podstawie art. 16 ust. 3 ustawy o ochronie danych osobowych, administrator danych odmawiający podpisania protokołu, może w terminie 7 dni przedstawić swoje stanowisko na piśmie Generalnemu Inspektorowi Ochrony Danych Osobowych.

Złożone zastrzeżenia i uwagi:

(należy umieścić wzmiankę zarówno o wniesieniu, jak i niewniesieniu zastrzeżeń i uwag)

W ciągu 7 dni od podpisania protokołu, zostaną złożone dodatkowe wyjaśnienia do jego treści.

.....

.....

.....

Oświadczam, że jeden egzemplarz protokołu kontroli został doręczony osobie reprezentującej podmiot kontrolowany.

Jednocześnie potwierdzam, iż wraz z ww. protokołem kontroli zostały przedstawione akta kontroli sygn. DIS-K-421/36/15, w tym załączniki do protokołu kontroli, oraz poinformowano o prawie wykonania kserokopii, odpisów i notatek z dokumentów znajdujących się w aktach kontroli, w szczególności wskazanych załączników.

MINISTER SPRAWIEDLIWOŚCI

Warszawa, 24-04-2015 r.

(miejscowość, data i podpis osoby reprezentującej podmiot kontrolowany)

Generalny Inspektor Kontroli