



**BIURO
GENERALNEGO INSPEKTORA
OCHRONY DANYCH OSOBOWYCH**

*Pan
Jacek Popiel
2007 11 12
795*

BIURO
GENERALNEGO INSPEKTORA
OCHRONY DANYCH OSOBOWYCH

2007 - 11 - 12

WPLYNEŁO

L.dz. Zał. 1

zob. zob

WPLYNEŁO DO BIURA BA

2007 - 11 - 12

BA

DIS-K-421/135/07

Protokół kontroli

W dniach 15 - 19 października 2007 r., na podstawie art. 14 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.), w celu kontroli zgodności przetwarzania danych z przepisami o ochronie danych osobowych, dokonano czynności kontrolnych w Ministerstwie Finansów z siedzibą w Warszawie przy ul. Świętokrzyskiej 12.

Z upoważnienia Generalnego Inspektora Ochrony Danych Osobowych czynności kontrolnych dokonali:

1. Jan Filipowicz – inspektor
legitymacja służbowa nr 161; upoważnienie nr 422/396/07
2. Krzysztof Staniak - inspektor
legitymacja służbowa nr 166; upoważnienie nr 422/397/07
3. Adam Myziak – inspektor
legitymacja służbowa nr 156; upoważnienie nr 422/398/07

Wykaz aktów prawnych dotyczących kontroli:

1. Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926 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), zwane dalej rozporządzeniem.

I. Ustalenia ogólne.

Ministerstwo działa na podstawie ustawy z dnia 4 września 1997 r. o działach administracji rządowej (Dz. U. z 2003 r. nr 159, poz. 1548 z późn. zm.); rozporządzenia Rady Ministrów z dnia 3 listopada 1999 r. w sprawie utworzenia Ministerstwa Finansów (Dz. U. nr 91, poz. 1020); rozporządzenia Prezesa Rady Ministrów z dnia 18 lipca 2006 r. w sprawie szczegółowego zakresu działania Ministra Finansów (Dz. U. nr 131, poz. 908 oraz Dz. U. nr 169, poz. 1204), a także zarządzenia nr 11 Prezesa Rady Ministrów z dnia 2 lutego 2007 r. w sprawie nadania statutu Ministerstwu Finansów (M.P. z 2007 r. Nr 9, poz. 98) oraz regulaminu organizacyjnego Ministerstwa Finansów (kopia regulaminu stanowi załącznik nr A1).

Zakresem kontroli objęto przetwarzanie danych osobowych w zakresie udostępniania danych osobowych przez Ministerstwo Finansów (dalej: MF).

II. Ustalenia szczegółowe.

Departament Administracji Podatkowej (AP).

Jak zeznała Pani Honorata Łopianowska, Zastępca Dyrektora Departamentu Administracji Podatkowej (protokół przesłuchania świadka stanowi załącznik nr A2), Krajowa Ewidencja Podatników funkcjonuje na podstawie art. 14 ustawy z dnia 13 października 1995 r. o zasadach ewidencji i identyfikacji podatników i płatników (tj. Dz. U. z 2004 r. Nr 269 poz. 2681 z późn. zm.). Krajowa Ewidencja Podatników (dalej: KEP) służy: gromadzeniu i weryfikacji danych wynikających ze zgłoszeń identyfikacyjnych i aktualizacyjnych podatników; porównaniu danych wynikających ze zgłoszeń identyfikacyjnych i aktualizacyjnych podatników z innymi rejestrami urzędowymi w celu ustalenia podatników, którzy naruszyli przepisy ustawy (art.14 ust. 2 ustawy o zasadach ewidencji i identyfikacji podatników i płatników) i jest prowadzona przez ministra właściwego do spraw finansów publicznych. KEP zawiera dane pochodzące ze zgłoszeń rejestracyjnych i aktualizacyjnych obejmujących m.in. takie informacje jak: numer NIP, imię i nazwisko podatnika, jego PESEL, dane o miejscu zamieszkania, właściwym urzędzie skarbowym. Departament AP udostępnia dane osobowe podatników i płatników z systemu informatycznego KEP uprawnionym podmiotom wskazanym w art. 15 ustawy o zasadach ewidencji i identyfikacji podatników i płatników (np. sądom, prokuraturom, organom celnym, organom podatkowym). Udostępnienie danych odbywa się na pisemny wniosek tych podmiotów. Dostęp do systemu informatycznego KEP posiadają wyłącznie wyznaczone uprawnione do tego osoby. Osoby te sporządzają odpowiedź dla danego wnioskodawcy. Zakres udostępnianych danych jest zależny od treści wniosków. Dane udostępniane są w związku ze sprawą prowadzoną przez danego wnioskodawcę, wniosek musi zawierać nr danej spraw (protokół przesłuchania świadka stanowi załącznik nr A3). Dostęp do wniosków oraz do odpowiedzi, przechowywanych w AP, mają Naczelnik Wydziału Krajowej Ewidencji Podatników oraz pracownicy Wydziału zajmujący się

rozpatrywaniem tych wniosków. Obieg ww. korespondencji odbywa się według zasad określonych w instrukcji kancelaryjnej (kopia instrukcji kancelaryjnej stanowi załącznik nr A4). Ww. dokumenty po zakończeniu dnia pracy są przechowywane w szafie zamykanej na klucz.

Jak zeznała Pani Honorata Łopianowska, Zastępca Dyrektora Departamentu Administracji Podatkowej, około jednego roku temu Centralne Biuro Antykorupcyjne (dalej: CBA) zwróciło się o udostępnienie przetwarzanych przez MF danych dotyczących podatników, zawierających informacje o ich rozliczeniach podatkowych. W związku z powyższym, miały miejsce spotkania podsekretarza Stanu Ministra Mariana Banasia z przedstawicielami CBA, dotyczące możliwości udostępnienia w sposób elektroniczny zasobów informatycznych resortu podległego Ministrowi Finansów. Na jednym ze spotkań minister polecił Pani Honoracie Łopianowskiej spotkanie się z przedstawicielami CBA w przedmiocie rozważenia możliwości udostępnienia danych w sposób elektroniczny, metodą teletransmisji dla CBA. Takie spotkania miały miejsce dwukrotnie w okresie letnim. Na spotkaniach analizowano możliwości udostępnienia danych podatników znajdujących się w zasobach informatycznych urzędów skarbowych. Podjęto decyzję, że w ramach Ministerstwa Finansów dokonana zostanie analiza prawna możliwości teletransmisji danych z systemów posiadanych przez administratorów danych w resorcie (urzędach skarbowych oraz Ministerstwie Finansów). Obecnie przedstawiciele CBA (Dyrektor Zarządu Postępowań Kontrolnych CBA albo agencji) zwracają się na piśmie, na podstawie art. 14 ust. 1 pkt 7 oraz art. 3 ustawy z dnia 9 czerwca 2006 r. o Centralnym Biurze Antykorupcyjnym (Dz. U. z 2006 r. Nr 104, poz. 708 z późn. zm.), w jednostkowych sprawach do Ministerstwa Finansów – Departamentu Administracji Podatkowej – Wydziału KEP, o przekazanie informacji i deklaracji podatkowych dotyczących konkretnych osób za wyraźnie wskazany czas. Pisma przesyłane są przesyłką poleconą. W celu udzielenia odpowiedzi dokonywane jest sprawdzenie danych podatnika, będącego obiektem zapytania CBA. Sprawdzenie realizowane jest przez jednego z trzech uprawnionych pracowników Wydziału KEP, którzy posiadają dostęp do bazy KEP. W odpowiedzi przekazywane są wystąpienia danej osoby w bazie KEP ze wskazaniem Urzędów Skarbowych, w których dana osoba dokonywała czynności wymagających złożenia deklaracji lub zeznania. Odpowiedź udzielania CBA nie zawiera innych danych poza tymi, które wskazane zostały we wniosku CBA, za wyjątkiem wskazania naczelników urzędów skarbowych właściwych dla tej osoby w okresie będącym przedmiotem zapytania. Z tych powodów Ministerstwo Finansów nie żąda upoważnień, o których mowa w rozporządzeniu Prezesa Rady Ministrów z dnia 23 listopada 2006 r. w sprawie wzoru imiennego upoważnienia funkcjonariusza Centralnego Biura Antykorupcyjnego stanowiącego podstawę udostępnienia danych osobowych (Dz. U. z 2006 r. Nr 215, poz. 1583). Odpowiedzi przesyłane są do CBA przesyłką poleconą, opatrzone klauzulą „tajemnica skarbową”. W MF pozostaje egzemplarz zapytania CBA i jeden egzemplarz pisma przewodniego MF. Obieg dokumentów dotyczących udostępnienia danych osobowych odbywa się zgodnie z instrukcją kancelaryjną. W Departamencie

nie opracowano odrębnej procedury dotyczącej postępowania z wnioskami o udostępnienie danych osobowych. Dokumentacja związana z wnioskiem przechowywana jest w Departamencie AP, w Wydziale KEP.

Ponadto, CBA występuje do Ministerstwa Finansów o umożliwienie korzystania z zasobów pozostających w dyspozycji naczelników urzędów skarbowych, zawartych w posiadanych przez nich systemach, obejmujących zasoby zawarte w systemach POLTAX oraz CZM. Udostępnienie wymienionych danych miałoby następować w sposób elektroniczny, bezpośrednio z zasobów danego systemu. Przedstawiciele CBA zwrócili się do Ministerstwa Finansów o dostęp do aplikacji RemDat, która pozwala na pobieranie danych z urzędów skarbowych. RemDat jest narzędziem funkcjonującym w resorcie na podstawie decyzji Ministra Finansów z 2003 r. nr 6/DI (kopia decyzji stanowi załącznik nr A5). Pozwala on sięgać do zawartości systemu POLTAX. Obecnie Ministerstwo Finansów nie przyznało CBA zdalnego dostępu do przetwarzanych danych, za pomocą teletransmisji, z uwagi na wątpliwości, czy istnieją ku temu podstawy prawne. W swoich wnioskach CBA powołuje się w tym zakresie na brzmienie przepisów ustawy o CBA, dokładnie na jej art. 22. Ponadto, w maju oraz lipcu 2007 r. z pisemnym wnioskiem o dostęp elektroniczny za pomocą teletransmisji zwróciła się także Służba Kontrwywiadu Wojskowego (dalej: SKW). Służba Kontrwywiadu Wojskowego nie wskazała w swoich pismach podstawy prawnej mającej uzasadniać udostępnienie danych. W związku z powyższym odmówiono udostępnienia danych. W następstwie tego wystąpienia odbyły się dwa spotkania robocze z przedstawicielami tej Służby, na których wskazywano brak możliwości udzielenia dostępu za pomocą teletransmisji danych do zasobów znajdujących się w dyspozycji naczelników urzędów skarbowych, z uwagi na konieczność posiadania przez osobę upoważnioną jednostkowego upoważnienia do konkretnego postępowania, według wzoru wynikającego z rozporządzenia Ministra Obrony Narodowej z dnia 25 września 2006 r. w sprawie wzoru pisemnego imiennego upoważnienia funkcjonariusza Służby Kontrwywiadu Wojskowego stanowiącego podstawę udostępnienia danych osobowych (Dz. U. z 2006 r. Nr 177, poz. 1312). Dotychczas Służba Kontrwywiadu Wojskowego nie zwróciła się o udostępnienie danych dotyczących podatników zawartych w zasobach POLTAX w urzędach skarbowych, lub w bazie KEP w Ministerstwie Finansów.

W toku kontroli ustalono, iż wnioski o udostępnienie danych wraz z egzemplarzami odpowiedzi przechowywane są w opisanych segregatorach, w obrębie których dokumenty poukładane są kolejno według daty wpływu wniosku. Segregatory przechowywane są w szafie drewnianej wyposażonej w zamek w pomieszczeniu nr 4321, znajdującym się na czwartym piętrze budynku przy ul. Świętokrzyskiej 12. Wejście do ww. pomieszczenia zabezpieczone jest drzwiami drewnianymi wyposażonymi w zamek mechaniczny (protokół oględzin stanowi załącznik nr A6).

Departament Kontroli Resortowej.

Jak zeznał Pan Rober Ścibek, Naczelnik Wydziału VIII w Departamencie Kontroli Resortowej (protokół przesłuchania świadka stanowi załącznik nr A7), Departament nie udostępniał danych osobowych CBA lub SKW, jak też żadnym innym podmiotom zewnętrznym. Departament udostępnia dane o podatnikach pochodzące z systemów informatycznych RemDat, KEP, PESEL, WEL jednostkom wykonującym zadania wywiadu skarbowego oraz ich jednostkom zamiejscowym, a także Wydziałowi Analiz i Planowania Urzędu Kontroli Skarbowej w Warszawie, oraz wydziałom MF wykonującym zadania z zakresu wywiadu skarbowego oraz wydziałom wykonującym zadania z zakresu kontroli resortowej (tylko z bazy RemDat i KEP) według procedury określonej w specjalnej instrukcji (kopia instrukcji 1/06 z dnia 10 lipca 2006 r. w sprawie korzystania przez pracowników Wywiadu Skarbowego z elektronicznych baz danych PESEL-NET, KEP, POLTAX, których końcówki znajdują się w Departamencie Kontroli Skarbowej II wraz z aneksami stanowi załącznik nr A8). Udostępnienie danych odbywa się na pisemny wniosek uprawnionego pracownika, podpisany przez jego przełożonego ze wskazaniem nr sprawy, w związku z którą następuje sprawdzenie. Istnieje wyraźny zakaz wykonywania sprawdzeń na ustne polecenie. Upoważniony pracownik Wydziału dokonuje sprawdzenia w oparciu o prawidłowo wypełniony wniosek i przygotowuje wydruk z baz. Wnioski, o których wyżej mowa są oznaczone klauzulą „zastrzeżone”. Wniosek oraz jeden egzemplarz pisma przewodniego wraz z wydrukami przesyłany jest do wnioskodawcy. W Wydziale pozostaje drugi egzemplarz pisma przewodniego oraz ewentualnie pismo przewodnie wnioskodawcy. Ponadto, prowadzony jest rejestr dokonanych sprawdzeń, w którym odnotowywane jest każde sprawdzenie. Wnioski oraz wydruki do momentu wysyłki są przechowywane w Kancelarii Materiałów Zastrzeżonych gdzie są zabezpieczone przed dostępem osób nieupoważnionych.

W toku kontroli ustalono, iż wnioski o udostępnienie danych wraz z wydrukami z przeszukanych baz danych są przechowywane w szafie pancерnej wyposażonej w zamek szyfrowy w pomieszczeniu nr 4412 – Kancelaria Materiałów Zastrzeżonych, znajdującym się na czwartym piętrze budynku przy ul. Świętokrzyskiej 12. Wejście do ww. pomieszczenia zabezpieczone jest drzwiami wzmocnionymi wyposażonymi w zamek mechaniczny oraz elektroniczny system kontroli dostępu (karta dostępu). W pomieszczeniu zainstalowano czujnik systemu alarmowego, pomieszczenie to posiada okratowane okna. Wejście z klatki schodowej na korytarz, z którego prowadzi wejście do ww. pomieszczenia jest zabezpieczone drzwiami otwieranymi przy pomocy karty dostępu, na ww. korytarzu zainstalowano czujniki systemu alarmowego oraz system kamer przemysłowych. Stacje komputerowe służące do przeszukiwania baz danych w związku z realizacją wniosków o udostępnienie danych znajdują się w pomieszczeniu nr 5201A znajdującym się na piątym piętrze budynku przy ul. Świętokrzyskiej 12. Wejście do ww. pomieszczenia prowadzi z pomieszczenia nr 5201, a wejście do pomieszczenia 5201 jest

zabezpieczone drzwiami plombowanymi klasy C, wyposażonymi w zamek oraz elektroniczny system kontroli dostępu. Ww. pomieszczenia posiadają okratowane okna, w pomieszczeniach zainstalowano czujniki systemu alarmowego, w pomieszczeniu nr 5201 znajduje się szafa pancerna. Wejście na piąte piętro z piętra czwartego zabezpieczone jest drzwiami wyposażonymi w elektroniczny system kontroli dostępu. Na klatce schodowej pomiędzy ww. piętrami zainstalowano kamery oraz czujniki systemu alarmowego (protokół oględzin stanowi załącznik nr A9).

Departament Kontroli Skarbowej.

Jak zeznał Pan Tomasz Korzecki, Naczelnik Wydziału Informatycznego Wspomagania Kontroli w Departamencie Kontroli Skarbowej (protokół przesłuchania świadka stanowi załącznik nr A10), Departament Kontroli Skarbowej nie udostępnia danych osobowych z systemów informatycznych RemDat i KEP podmiotom zewnętrznym, gdyż nie jest ich właścicielem. Dotychczas nie były rozpatrywane wnioski o udostępnienie danych Centralnemu Biuru Antykorupcyjnemu lub Służbie Kontrwywiadu Wojskowego. Dotychczas rozpatrywany był jeden wniosek o udostępnienie danych osobowych podatnika pochodzący z sądu. Wniosek ten dotyczył udostępnienia danych dotyczących aktualnego adresu miejsca zamieszkania podatnika. Departament Kontroli Skarbowej w odpowiedzi na ww. wniosek skierował wnioskodawcę by zwrócił się o udzielenie informacji do naczelnika właściwego urzędu skarbowego ze względu na miejsce zamieszkania tego podatnika, które było wskazane w piśmie tego sądu. Pismo (wniosek) wraz z udzieloną odpowiedzią są przechowywane w Wydziale. Dostęp do ww. dokumentów mają wyłącznie osoby upoważnione. Ww. dokumenty przechowywane są w szafie wyposażonej w zamek. Udostępnianie danych osobowych z ww. systemów w ramach Departamentu odbywa się zawsze na pisemny wniosek pracownika zatwierdzony przez Naczelnika Wydziału, w którym dany pracownik pracuje (formularze wniosków o udostępnienie danych osobowych stanowią załącznik nr A11). Na udostępnienie danych wyraża zgodę Naczelnik Wydziału Informatycznego Wspomagania Kontroli. Upoważniony pracownik Wydziału opracowuje odpowiedź, która za pismem przewodnim przekazywana jest do rąk własnych wnioskodawcy. W Wydziale pozostaje wniosek wraz z kopią pisma przewodniego. Dostęp do ww. pism posiadają upoważnieni pracownicy Wydziału. Dokumentacja ta przechowywana jest w szafie wyposażonej w zamek. Dostęp do systemu informatycznego RemDat posiadają upoważnieni pracownicy Departamentu, którzy wykorzystują ww. dostęp do realizacji bieżących potrzeb służbowych. System informatyczny RemDat umożliwia zdalne połączenie się z bazami systemu POLTAX we wszystkich urzędach skarbowych w Polsce. Zapytanie realizowane jest poprzez zdefiniowane skrypty, które określają zakres pobieranych informacji. System RemDat umożliwia jedynie pobieranie danych z systemu

POLTAX natomiast nie umożliwia pobierania danych z innych systemów informatycznych znajdujących się w urzędach skarbowych.

W toku kontroli ustalono, iż wnioski o udostępnienie danych wraz z pismami przewodnimi Wydziału są przechowywane w pomieszczeniu nr 4149 znajdujących się na czwartym piętrze budynku. Ww. dokumenty umieszczono w segregatorach w drewnianej szafie wyposażonej w zamek. Do ww. pomieszczenia prowadzi przejście z pomieszczenia nr 4148. Wejścia z korytarza do ww. pomieszczeń zabezpieczone są drzwiami drewnianymi wyposażonymi w zamek (protokół oględzin stanowi załącznik nr A12).

Jak zeznał Pan Paweł Szyfter, Naczelnik Wydziału Operacyjnego Departamentu Kontroli Skarbowej I (protokół przesłuchania świadka stanowi załącznik nr A13), Wydział posiada dostęp do systemu informatycznego RemDat, który wykorzystywany jest do prowadzenia ustawowych niejawnych czynności operacyjno-rozpoznawczych. Dotychczas nie było przypadku przekazywania informacji podatkowych z baz danych podatkowych żadnym organom, w tym Centralnemu Biuru Antykorupcyjnemu, Służbie Kontrwywiadu Wojskowego. W tym zakresie wydany został okólnik obligujący do prawnego zachowania wszystkich pracowników wywiadu skarbowego w zakresie udostępniania informacji podatkowej (kopia ww. okólnika oraz wzoru pisma o odmowie udzielenia informacji stanowią załącznik nr A14). W Wydziale opracowano „Instrukcję w sprawie korzystania przez pracowników Wydziału Operacyjnego z elektronicznych baz danych, których końcówki znajdują się w Wydziale Operacyjnym Departamentu Kontroli Skarbowej I” (kopia ww. instrukcji stanowi załącznik nr A15).

Departament Podatków i Opłat Lokalnych (PL).

Jak zeznała Pani Justyna Przekopiak, Dyrektor Departamentu Podatków i Opłat Lokalnych (protokół przesłuchania świadka stanowi załącznik nr A16), w Departamencie nie są przetwarzane dane osobowe podatników, w związku z postępowaniami podatkowymi. Centralne Biuro Antykorupcyjne ani Służba Kontrwywiadu Wojskowego nie zwracały się do Departamentu z żadnymi wnioskami o udostępnienie danych osobowych, inne instytucje zewnętrzne również nie zwracały się o udostępnienie danych. System Czynności Majątkowych (CZM) – służy do weryfikacji wartości nieruchomości dla celów podatków majątkowych, w systemie tym przetwarzane są dane osobowe podatników. Departament PL nie ma dostępu do danych przetwarzanych w tym systemie. System CZM nie jest scentralizowany, działa na poziomie poszczególnych urzędów skarbowych. Inne komórki organizacyjne MF nie posiadają dostępu on-line do danych osobowych podatników przetwarzanych w ww. systemie (kopia zarządzenia nr 1/07 Dyrektora Departamentu Podatków i Opłat Lokalnych z dnia 25 maja 2007 r. w sprawie wprowadzenia wewnętrznego regulaminu organizacyjnego dla Departamentu Podatków i Opłat Lokalnych wraz z kopią regulaminu stanowią załącznik nr A17).

Zabezpieczenia ogólne.

Jak wyjaśnił Pan Kazimierz Winiecki, Naczelnik Wydziału Ochrony, Spraw Obywatelskich i Obrony Cywilnej Biura Logistyki (protokół przyjęcia ustnych wyjaśnień stanowi załącznik nr A18), Budynek Ministerstwa Finansów jest chroniony całodobowo przez Wewnętrzną Służbę Ochrony Ministerstwa Finansów. Ministerstwo Finansów posiada Plan Ochrony zatwierdzony przez Komendanta Stołecznego Policji. Przy wszystkich wejściach do gmachu budynku Ministerstwa Finansów są zainstalowane tzw. „kołowrotki” oraz czytniki wejść i wyjść. Każdy pracownik Ministerstwa posiada indywidualny identyfikator upoważniający go do wejścia i wyjścia z budynku Ministerstwa. Interesanci i goście mogą wchodzić i wychodzić z budynku Ministerstwa jedynie wejściem głównym od ul. Świętokrzyskiej 12. Goście specjalni np. Ministrowie, wojewodowie nie są poddawani kontroli. Natomiast pozostałe osoby są rejestrowane w systemie elektronicznym, a po godzinie 16 - tej w rejestrze prowadzonym w formie papierowej oraz poddawane są kontroli na obecność niebezpiecznych materiałów i narzędzi. Zarówno wewnątrz jak i na zewnątrz budynku zainstalowano kamery, z których obraz przekazywany jest do Alarmowego Centrum Odbioru, gdzie całodobowo pełni służbę dyżurny wartownik. Obraz z ww. kamer (szt. 32) jest rejestrowany i podglądany na monitorach. W budynku Ministerstwa zainstalowano system alarmowy. W wybranych strefach zainstalowano czujniki systemu alarmowego, we wszystkich pomieszczeniach zainstalowano czujniki ppoż. W budynku znajdują się strefy bezpieczeństwa oraz strefy ograniczonego dostępu, gdzie uprawnienia do tych stref nadaje administrator danej strefy. Wstęp do strefy odbywa się przy użyciu elektronicznej karty dostępu. Użycie kart dostępu jest rejestrowane w systemie elektronicznym. Wybrane pomieszczenia są zabezpieczane plombą tzw. referentką. Klucze do niektórych pomieszczeń są pozostawiane w wartowni w specjalnym plombowanym pojemniku. Zdanie i pobieranie kluczy jest odnotowane w stosownym rejestrze. Pomieszczenia plombowane są sprzątane w obecności pracowników, pozostałe pomieszczenia sprzątane są poza godzinami pracy pracowników Ministerstwa Finansów.

Dokonano kontroli systemów informatycznych służących do przetwarzania danych osobowych oraz ich zabezpieczeń.

Jak wyjaśniła Pani Anna Małysa, Specjalista w Departamencie Eksploatacji Systemów Informatycznych – EI) (protokół przyjęcia ustnych wyjaśnień stanowi załącznik nr B17), w Ministerstwie Finansów nadzór nad bezpieczeństwem przetwarzania danych osobowych pełni Pan Tadeusz Wydra, Dyrektor Generalny Ministerstwa Finansów (kopia upoważnienia stanowi załącznik nr B1).

W kontrolowanej jednostce wdrożono następujące dokumenty:

- „Polityka Bezpieczeństwa Informacji Dokument Główny” (załącznik nr B2),
- „Polityka Bezpieczeństwa Grupy Danych Osobowych” (załącznik nr B3),

- „Instrukcja Postępowania w Sytuacji Naruszenia Bezpieczeństwa Danych Osobowych”, (załącznik nr B4)
- „Polityka bezpieczeństwa danych osobowych w systemie informatycznym” (załącznik nr B13),
- „Polityka bezpieczeństwa danych osobowych – Instrukcja zarządzania systemem informatycznym” (załącznik nr B14).

W kontrolowanej jednostce prowadzony jest wykaz „Użytkownicy w zakresie KONTROLA” (załącznik nr B5). Ewidencję użytkowników dopuszczonych do przetwarzania danych osobowych za pośrednictwem systemu RemDat stanowi zbiór „Wniosków o dostęp do baz POLTAX urzędów skarbowych poprzez centralny system zdalnego wykonywania raportów RemDat” (załącznik nr B6). Wspomniane wnioski przechowywane są przez Panią Annę Małyse, w zamykanej szafie. Zawierają one upoważnienie do przetwarzania danych za pomocą systemu RemDat. Przebywanie osób nieuprawnionych w obszarze przetwarzania danych w Ministerstwie Finansów dopuszczalne jest za zgodą administratora danych lub w obecności osoby upoważnionej do przetwarzania danych osobowych.

Zarządzanie hasłami dostępu do systemu RemDat odbywa się dla użytkowników w budynku Ministerstwa Finansów, w taki sposób, że całość hasła do systemu jest przekazywana w momencie instalacji aplikacji klienckiej na stacji roboczej użytkownika. W wypadku użytkowników spoza budynku Ministerstwa jednocześnie z przekazaniem wniosku do akceptacji, przyszły użytkownik określa swoje standardowe hasło do systemu. Powyższe hasło użytkownik powinien czytelnie wpisać na kserokopii wniosku (załącznik nr B6), w pkt nr 8. Kopia wniosku umieszczana jest w kopercie opisanej w odpowiedni sposób, zaklejonej i umieszczanej w kolejnej kopercie zaadresowanej do Departamentu Eksploatacji Systemów Informatycznych (EI), po czym wysyłana jest listem poleconym. Pierwsze logowanie do systemu możliwe jest po podaniu hasła składającego się ze standardowego hasła, uzupełnionego o drugą część, która będzie przekazana użytkownikowi wraz z jego identyfikatorem w systemie. Przy pierwszym logowaniu system żąda zmiany hasła na nowe. W wypadku zapomnienia hasła przez użytkownika niezbędne jest pisemne wystąpienie Dyrektora danej jednostki do Departamentu EI, z prośbą o zmianę hasła, zawierające: nr referencyjny wniosku o dostęp, imię i nazwisko użytkownika oraz aktualny nr telefonu. Telefoniczne prośby zmiany hasła nie są uwzględniane. W przypadku zablokowania konta użytkownika w RemDat, Dyrektor jednostki, która złożyła wniosek o dostęp, jest zobowiązany do niezwłocznego poinformowania Departamentu EI o ustaniu okoliczności uprawniających wskazaną we wniosku osobę do korzystania z systemu RemDat.

System informatyczny RamDat.

System RemDat stanowi narzędzie programowe przeznaczone do zdalnego dostępu do danych przetwarzanych w bazach POLTAX urzędów skarbowych. Do obsługi systemu RemDat nie są wykorzystywane komputery przenośne.

W kontrolowanej jednostce wymagania techniczno-organizacyjne jakie muszą być spełnione dla systemu RemDat określone zostały w następujących dokumentach:

- „Dokumentacja techniczno-użytkowa systemu RemDat. Administracja serwerem danych w urzędzie skarbowym” (załącznik nr B7),
- „Dokumentacja techniczno-użytkowa systemu RemDat. Aplikacja klienta systemu RemDat” (załącznik nr B8),
- „Wymagania techniczne i konfiguracyjna stacji roboczej klienta systemu RemDat” (załącznik nr B9),
- „Konfiguracja sieci WAN dla systemu RemDat” (załącznik nr B10),
- „System RemDat – wnioskowanie o dostęp do baz POLTAX urzędów skarbowych” (załącznik nr B11).

W dokumencie „System RemDat – wnioskowanie o dostęp do baz POLTAX urzędów skarbowych” opisane zostały procedury określające sposób uzyskania dostępu do POLTAX przy użyciu RemDat. Uzyskanie dostępu do systemu POLTAX wymaga wypełnienia „Wniosku o dostęp do baz POLTAX urzędów skarbowych poprzez centralny system zdalnego wykonywania raportów RemDat”, którego wzór określony został w załączniku do Decyzji Ministra Finansów nr 6/DI z dnia 8 lipca 2003 r., w sprawie dostępu do informacji w bazach systemu POLTAX urzędów skarbowych (załącznik nr B12). Dyrektor jednostki zatrudniającej osobę ubiegającą się o dostęp do bazy POLTAX przesyła wypełniony wniosek do Departamentu Eksploatacji Systemów Informatycznych. Wniosek powinien zawierać:

- pieczętę jednostki,
- nr referencyjny wniosku (zgodny z instrukcją kancelaryjną danej jednostki), miejscowość i datę,
- dane jednostki zgłaszającej wniosek (pełna nazwa),
- dane użytkownika,
- informacje o stacji roboczej użytkownika,
- uzasadnienie wniosku, w wypadku wnioskowania o dostęp z wykonywaniem raportów zawierających dane podlegające tajemnicy skarbowej lub ochronie danych osobowych należy podać także podstawę prawną,
- określenie zakresu dostępu (wszystkie urzędy lub urzędy podlegające wskazanej izbie skarbowej),

- określenie uprawnień dostępu (bez prawa lub z prawem wykonywania raportów z danymi podlegającymi tajemnicy skarbowej lub ochronie danych osobowych),
- datę, podpis i imienną pieczętkę Dyrektora jednostki składającej wniosek.

Jak wyjaśniła Anna Małysa (protokół przyjęcia ustnych wyjaśnień stanowi załącznik nr B18), dostęp do danych przetwarzanych w bazach POLTAX urzędów skarbowych, poprzez system RemDat do dnia kontroli posiadały wyłącznie Ministerstwo Finansów, Izby Skarbowe oraz Urzędy Kontroli Skarbowej.

Użytkownik może korzystać z systemu RemDat wyłącznie z jednej stacji roboczej, która została mu przypisana do tego celu. Wymagania techniczne dla stacji zależą od uprawnień użytkownika, któremu dana stacja została przypisana. Minimalne wymagania dla stacji z RemDat są następujące:

- system Ms Windows RAM min 64MB (dla Windows 98) i min. 128 MB dla (Windows NT, Windows 2000), procesor Pentium 300 MHz,
- zabezpieczenie hasłem konta na poziomie systemu operacyjnego stacji roboczej,
- stacja podłączona do sieci LAN Ministerstwa Finansów (dla stacji wewnątrz MF), lub do resortowej sieci WAN ze statycznym adresem IP (dal stacji spoza MF).

Stacje robocze użytkowników posiadających prawo wykonywania raportów z danymi podlegającymi tajemnicy skarbowej lub ochronie danych osobowych spełniają wymagania dla systemów informatycznych przeznaczonych do przetwarzania takich danych, a w szczególności:

- znajdują się w wydzielonym pomieszczeniu, do którego dostęp mają wyłącznie osoby upoważnione,
- wykorzystywane są wyłącznie przez użytkowników systemu RemDat, którym zostały przypisane,
- zabezpieczone są hasłem na poziomie BIOS,
- pracują pod kontrolą systemów operacyjnych z systemem plików NTFS (Windows NT, Windows 2000),
- drukarka służąca do wydruków zlokalizowana jest w tym samym pomieszczeniu, w którym znajduje się stacja robocza,
- konta lokalne użytkownika spełniają następujące założenia:
 - o grupa konta z uprawnieniami maksymalnie „Użytkownicy”,
 - o restrykcje nałożone na hasło: okres ważności hasła nie przekracza 30 dni, minimalny okres ważności hasła 1 dzień, minimalna długość hasła 8 znaków, unikalność hasła do 5 wstecz, blokada konta po 3 nieudanych próbach logowania, czas trwania blokady 30 min., zabezpieczony hasłem wygaszacz ekranu włączany po 5 min nieaktywności użytkownika,

- o stacje działają w wydzielonej sieci umożliwiającej dostęp wyłącznie do serwerów POLTAX i serwera identyfikacyjnego RemDat, bez dostępu do internetu, poczty elektronicznej i zasobów dyskowych innych stacji.

W celu pobrania za pomocą systemu RemDat danych z baz urzędu skarbowego pracownik prowadzący sprawę i nie mający dostępu do omawianego systemu zobowiązany jest przedłożyć pisemny wniosek ze wskazaniem nazwy raportu, urzędu skarbowego, identyfikatora podmiotu oraz zakresu danych, który ma zostać pobrany. Na podstawie takiego wniosku podejmowane są czynności mające na celu uzyskanie wskazanych informacji z baz urzędów skarbowych. Następnie dane przekazywane są w formie elektronicznej lub papierowej, za pokwitowaniem, do osoby wnioskującej. Odpowiedź udzielana jest w jednym egzemplarzu.

Pracownicy Departamentu EI wykorzystują system RemDat do celów technicznych, takich jak np. sprawdzanie tworzenia kopii awaryjnych w urzędach skarbowych. Lista skryptów zdefiniowanych w RemDat przedstawiona została w załączniku nr B15. Pełny opis wykonywanych skryptów stanowi załącznik nr B16.

Każdorazowa sesja wykonywana poprzez RemDat na bazach Poltax zapisywana jest w logach, w pliku historii o nazwie RemDatSrv.log, w urzędach skarbowych. We wspomnianym pliku odnotowywane są następujące informacje: adres IP, nazwa klienta, data (data rozpoczęcia sesji), status (kod zakończenia sesji), opis (krótki komentarz – tekst poprawnie wykonanego polecenia, wraz z użytymi parametrami lub komunikat błędu). Ponadto, każdy skrypt nadesłany przez użytkownika (Klient RemDat) zapisywany jest w katalogu serwera postawionego w urzędzie skarbowym. Na podstawie pliku RemDatSrv.log oraz zawartości zapisanego skryptu administrator systemu operacyjnego w urzędzie skarbowym może określić kto, kiedy i jakie dane pobrał z lokalnej bazy.

Jak wyjaśnił Pan Sławomir Flis, Specjalista w Departamencie Eksploatacji Systemów Informatycznych (protokół przyjęcia ustnych wyjaśnień stanowi załącznik nr B19), dane użytkowników systemu RemDat, w tym adresy stacji roboczych i zakres dostępu podawane są każdorazowo w załączniku do pisma kierowanego do Departamentu Eksploatacji Systemów Informatycznych, zlecającego instalację zestawu RemDat w urzędach skarbowych. Zakres dostępu określony jest symbolicznie przez czteroznakową maskę kodów urzędów skarbowych, gdzie pierwsze dwa znaki wyznaczają dostęp do województwa (kod IS), a dwa ostatnie dostęp do poszczególnych urzędów skarbowych (kod US). Szczegóły konfiguracji sieci WAN opisane zostały w dokumencie „Konfiguracja sieci WAN dla systemu RemDat” (załącznik nr B10).

Dostęp do baz Poltax poprzez wykorzystanie systemu RemDat możliwe jest poprzez dokonanie autoryzacji na poziomie centralnego serwera identyfikacyjnego RemDatIds, zlokalizowanego w siedzibie Ministerstwa Finansów, w serwerowni 157 oraz na poziomie

serwera RemDatSrv, zlokalizowanego w konkretnym urzędzie skarbowym. Serwer RemDatSrv pełni rolę serwera danych systemu RemDat w urzędzie skarbowym. Zadaniem programu jest nasłuch (oczekiwanie na zlecenie) oraz wykonanie procedury pobrania określonych danych z bazy POLTAX i przesłania ich do upoważnionego klienta (aplikacja zainstalowana na stacji roboczej użytkownika). Dane z lokalnej bazy pobierane są za pomocą skryptów SQL wykonywanych w kontekście użytkownika RDOOnly. Wszelkie transmisje wyników zapytań poprzez sieć są kodowane. Szczegółowe informacje na temat działania serwera RemDatSrv zamieszczone zostały w dokumencie „Dokumentacja techniczno użytkowa systemu RemDat. Administracja serwerem danych w urzędzie skarbowym” (załącznik nr B7).

Klient RemDat – aplikacja klienta systemu RemDat.

Aplikacja o nazwie „Klient RemDat” pełni rolę programu klienta w systemie RemDat. Aplikacja przeznaczona jest do użytku w środowisku systemów operacyjnych Windows 98/NT/2000. Czynności użytkownika sprowadzają się do prostych, interaktywnych operacji na standardowych elementach systemu Windows (przyciski, okienka edycyjne, plansze dialogowe). Typowa sesja klienta obejmuje następujące kroki:

- uruchomienie programu – poprzez menu Start/Programy/DI MF i wybór aplikacji „Klienta RemDat”,
- rejestracja użytkownika w systemie – podanie hasła dostępu do systemu RemDat, a następnie potwierdzenie poprzez „Enter”. Po upływie ważności hasła system żąda podania nowego hasła (po 4 tygodniach). Pomyślna rejestracja w systemie sygnalizowana jest komunikatem „Klient zarejestrowany w systemie – O.K.”,
- wybór właściwej procedury – wybór jednej z dostępnych, identyfikowanych przez opis programu procedur pobierania danych,
- lokalizacja wykonania procedury – wskazanie na liście dostępnych serwerów danych miejsca, z których będą pobierane dane. Lista serwerów uporządkowana jest według kodów urzędów, w których pierwsze dwie cyfry określają kod województwa. Zaznaczanie odbywa się w sposób addytywny – kolejny element dodawany jest do elementów wybranych uprzednio. Ponowne wskazanie tego samego elementu (uprzednio wskazanego) powoduje anulowanie zaznaczenia. Wyboru serwerów danych można dokonywać grupowo (województwami). W tym celu należy wskazać na rozwijanej liście (poniżej listy serwerów) opis grupy – w szczególnym przypadku wybrać można „wszystkie” lub „żaden”,
- rozpoczęcie wykonywania procedury – wybranie przycisku „Start”, podanie wartości ewentualnych parametrów wykonywania procedury oraz określenie, czy dane mają być

dopisane do pobranych wcześniej, czy też ewentualnie istniejące dane mają być nadpisane (właściwe okna dialogowe otwierane są automatycznie przez program),

- oczekiwanie na wyniki – realizacja procedury na serwerach danych jest na bieżąco monitorowana przez program. W okienku komunikatów wyświetlany jest procent realizacji przebiegu, a po zakończeniu wszystkich zdalnych sesji pojawia się komunikat „przebieg zakończony”,
- odczyt wyników – w celu uzyskania informacji o przebiegu konkretnej sesji należy wskazać wymaganą pozycję na liście serwerów (lub odpowiadający danej pozycji punkt na mapie). Jeśli sesja zakończyła się błędem wyświetlany jest komunikat o przyczynie błędu. Jeśli sesja przebiegła pomyślnie to komunikat zostanie wyświetlony na ekranie (pierwsze 65kB tekstu), a naciśnięcie przycisku „Edycja” umożliwi pełną obróbkę tekstu raportu w programie „WordPad”,
- przygotowanie do kolejnego przebiegu – należy wskazać na rozwijalnej liście grup serwerów pusty wiersz oznaczający wybór „żaden”, co pozwala na rozpoczęcie kolejnej procedury pobierania danych,
- zakończenie pracy programu – następuje poprzez wybór przycisku „x”, w prawym górnym rogu okna programu.

Oprócz opisanych powyżej rutynowych czynności użytkownik powinien w trakcie pierwszego uruchamiania, określić konfigurację programu, w ramach instalacji aplikacji „Klient RemDat”. W tym celu należy podać numer portu TCP, adres IP serwera identyfikacyjnego oraz nazwę klienta. Dwa pierwsze elementy są takie same dla wszystkich użytkowników systemu RemDat, trzeci jest unikalny dla każdego klienta. Dokładny opis aplikacji „Klient RemDat” znajduje się w dokumencie „Dokumentacja techniczno-użytkowa systemu RemDat. Aplikacja klienta systemu RemDat” (załącznik nr B8).

Uzyskanie dostępu do systemu RemDat wymaga zalogowania się na konto lokalne w systemie operacyjnym. Po zalogowaniu się użytkownik ma dostęp wyłącznie do dysku F, nie ma dostępu do Internetu, poczty elektronicznej i zasobów sieci resortowej Ministerstwa Finansów, a także nie może udostępniać własnych zasobów. Po zalogowaniu się na stację roboczą użytkownika, który nie jest upoważniony do użytkowania systemu RemDat, dysk F nie jest dla niego widoczny. Na kontrolowanej stacji, po 5 min. nieaktywności użytkownika w systemie uruchamiany jest zabezpieczony hasłem wygaszacz ekranu. Na stacji roboczej zainstalowany jest program antywirusowy Trend Micro Office Scan Client. Użytkownik logujący się na konto lokalne z dostępem do RemDat nie ma możliwości zmiany parametrów oraz uprawnień konta. Katalog tymczasowy umieszczany jest na macierzystym dysku tymczasowym użytkownika. Na kontrolowanej stacji roboczej zainstalowane są skrypty dotyczące kontroli. Na stacji roboczej nie

znaleziono wyników działania skryptów. Protokoły oględzin systemu RemDat stanowią załączniki nr B21 i B22.

System informatyczny KEP (Krajowa Ewidencja Podatników).

Jak wyjaśnił Pan Dariusz Morawski, (protokół przyjęcia ustnych wyjaśnień stanowi załącznik nr B20), w Krajowej Ewidencji Podatników (KEP) przetwarzane są informacje rejestrowe dotyczące wszystkich podatników. Omawiana baza zlokalizowana jest fizycznie na serwerze w Ministerstwie Finansów, w sieci izolowanej od sieci publicznej. Baza zasilana jest przez urzędy skarbowe drogą elektroniczną poprzez przesłanie danych w zaszyfrowanej formie, na serwer wykorzystywany w Ministerstwie Finansów do wymiany danych z urzędami skarbowymi, a następnie dane te przenoszone są ręcznie za pomocą tasiemek na serwer bazy danych KEP. Baza jest zasilana z tasiemek poprzez skrypt ładujący dane.

Dostęp do bazy możliwy jest wyłącznie z siedziby Ministerstwa Finansów, dla osób upoważnionych przez Departament Administracji Podatkowej. Bezpośredni dostęp do danych możliwy jest poprzez podanie indywidualnego identyfikatora użytkownika oraz odpowiadającego mu hasła. Każdemu użytkownikowi nadano ograniczone uprawnienia, umożliwiające wyłącznie wykonywanie przydzielonych mu zadań służbowych.

Każdorazowy dostęp do bazy odnotowywany jest w formie papierowej w zakresie data, godzina, wejścia i wyjścia do pomieszczenia, w którym się znajduje stacja robocza z dostępem do KEP (stacje dostępu do KEP znajdują się w strefach zamkniętych), podstawa prawna dostępu do informacji z KEP (nr pisma/nr sprawy). Każdorazowe zalogowanie się użytkownika do bazy odnotowywane jest w logach systemowych.

Dane przetwarzane w KEP nie są udostępniane online instytucjom zewnętrznym. Udostępnianie danych odbywa się poprzez pisemne wystąpienie instytucji uprawnionej o zgodę do Administratora Danych Osobowych z Departamentu Administracji Podatkowej (AP). W przypadku, gdy zgoda na udostępnienie danych zostanie udzielona, dane z bazy pobierane są przez uprawnionego pracownika MF i przekazywane na nośniku informacji typu dyskietka lub płyta do AP, a następnie do wnioskodawcy. W bazie KEP nie są odnotowywane informacje komu, kiedy, w jakim celu i zakresie dane zostały udostępnione. Dane z bazy KEP nie są udostępniane odbiorcom danych w rozumieniu art. 7 pkt 6 ustawy o ochronie danych osobowych.

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:

.....

.....

.....

.....

.....

.....

.....

.....

Niniejszy protokół sporządzono w dwóch jednobrzmiących egzemplarzach.

Warszawa, dnia 6 listopada 2007 r.

Z upoważnienia Ministra Finansów
DYREKTOR GENERALNY

Tadeusz Wydra

(data, podpis i pieczęć osoby
reprezentującej podmiot kontrolowany)

Jan Filipowicz
Krzysztof Staniak
A. M. R.

(podpisy kontrolujących)

12/11/2007