Warszawa, dn. 18.12.2017 r.

Rafał Rogala
Szef Urzędu do Spraw Cudzoziemców

BSZ.WKIN.091.3.2017

PROTOKÓŁ KONTROLI

Na podstawie art. 455 ust. 1 ustawy z dnia 12 grudnia 2013 r. *o cudzoziemcach* (t.j. Dz. U. z 2017 r. poz. 2206 z późn. zm.) w związku z § 5 pkt. 3 i § 7 ust. 3 rozporządzenia Ministra Spraw Wewnętrznych z dnia 24 kwietnia 2014 r. *w sprawie kontroli korzystania z dostępu do danych przetwarzanych w krajowym zbiorze rejestrów, ewidencji i wykazu w sprawach cudzoziemców za pomocą urządzeń telekomunikacyjnych lub systemów teleinformatycznych* (Dz. U. z 2014 r. poz. 551) kontrolę w Wydziale Spraw Cudzoziemców Mazowieckiego Urzędu Wojewódzkiego (dalej WSC MUW) położonego przy ul. Marszałkowskiej 3/5 w Warszawie przeprowadził zespół kontrolny w składzie:

- **Bartosz Koneczny,** Naczelnik Wydziału Kontroli i Nadzoru w Biurze Szefa Urzędu, upoważnienie nr 18/2017 – kierownik zespołu kontrolnego,
- , Administrator Bezpieczeństwa Informacji w Urzędzie do Spraw Cudzoziemców, upoważnienie nr 17/2017 – członek zespołu kontrolnego,
- , podreferendarz w Biurze Informatyki Urzędu do Spraw Cudzoziemców, upoważnienie nr 16/2017 – członek zespołu kontrolnego.

Kierownikiem podmiotu kontrolowanego w okresie poddanym kontroli był Wojewoda Mazowiecki, Pan Zdzisław Sipiera, który jako osobę do kontaktu z zespołem kontrolnym wyznaczył Dyrektor Wydziału Spraw Cudzoziemców Mazowieckiego Urzędu Wojewódzkiego w Warszawie, Panią Izabelę Szewczyk[1].

Przedmiotem kontroli była realizacja przez uprawniony podmiot wskazany w art. 450 ust. 1 pkt. 1 ustawy o cudzoziemcach, jakim jest Wojewoda Mazowiecki, warunków określonych w art. 453 ustawy, umożliwiających udostępnianie danych przetwarzanych w krajowym zbiorze rejestrów, ewidencji i wykazu w sprawach cudzoziemców[2] za pomocą urządzeń telekomunikacyjnych, a w szczególności spełnianie przez Wojewodę Mazowieckiego warunków określonych w art. 453 ust. 1 i 2 ustawy, w okresie od 1 maja do 31 października 2017 r.

[1] pismo nr WSC-VI.1610.2.2017 z dnia 17 listopada 2017 r.
[2] dalej KZR

Podczas oceny[3] spełniania przez kontrolowany podmiot określonych we wskazanym wyżej przepisie warunków zespół kontrolny weźmie pod uwagę następujące kategorie:

1. Stosowane zabezpieczenia techniczne i organizacyjne odpowiednie do przetwarzania danych osobowych, w szczególności uniemożliwiające dostęp do przetwarzania danych osobowych i wykorzystywania danych niezgodnie z celem ich uzyskania.
2. Stosowane zabezpieczenia urządzeń telekomunikacyjnych lub systemów teleinformatycznych przeznaczonych do komunikowania się z KZR.

Pismem z dnia 2 maja 2014 r. Wojewoda Mazowiecki wystąpił do Szefa Urzędu do Spraw Cudzoziemców[4] z wnioskiem na podstawie art. 454 ust. 1 ustawy o cudzoziemcach o wyrażenie zgody na udostępnianie danych przetwarzanych w KZR za pomocą urządzeń telekomunikacyjnych na potrzeby postępowań prowadzonych przez ten organ na podstawie przepisów ustawy o cudzoziemcach. Organ wnioskujący oświadczył, że:

- posiada odpowiednio zabezpieczone urządzenia telekomunikacyjne lub systemy teleinformatyczne przeznaczone do komunikowania się z KZR;
- posiada zabezpieczenia techniczne i organizacyjne odpowiednie do przetwarzania danych osobowych w szczególności uniemożliwiające dostęp osób nieuprawnionych do przetwarzania danych osobowych i wykorzystywania danych niezgodnie z celem ich uzyskania;
- wykonuje zadania, których specyfika lub zakres uzasadniają uzyskanie danych tą drogą.

Decyzją z dnia 6 maja 2014 r. nr 9/2014 Szef Urzędu wyraził zgodę Wojewodzie Mazowieckiemu na udostępnianie danych przetwarzanych w KZR za pomocą urządzeń telekomunikacyjnych.

Według stanu na dzień 6 listopada 2017 r. w podmiocie podlegającym kontroli aktywne były 284 konta użytkowników indywidualnych KZR.

W toku kontroli zespół kontrolny pobierał pisemne wyjaśnienia[5] oraz dokonał oględzin w siedzibie Wydziału Spraw Cudzoziemców Mazowieckiego Urzędu Wojewódzkiego[6] w której zlokalizowane są stanowiska dostępowe do KZR[7]. W czasie kontroli ustalono, iż osoby uzyskujące dostęp do KZR zapoznały się z *Polityką Bezpieczeństwa Danych Osobowych Urzędu do Spraw Cudzoziemców* oraz *Instrukcją Zarządzania Systemem Teleinformatycznym POBYT v.2 poziom podwyższony* nr WBIOIN.270.5.2017/DM z dnia 21 marca 2017 r. Papierowa wersja tej dokumentacji znajduje się w pok. 404, dodatkowo dokumentacja ta umieszczona jest na wydzielonym w tym celu dysku, do którego dostęp ze swojego komputera ma każdy pracownik WSC MUW. O każdej zmianie w dokumentacji użytkownicy informowani są za pośrednictwem poczty elektronicznej

[3] zastosowano 3-stopniową skalę ocen: pozytywna, pozytywna z nieprawidłowościami, negatywna
[4] dalej UdSC
[5] pismo nr WSC-VI.1234.72.2017 z dnia 29 listopada 2017 r.
[6] dalej WSC MUW
[7] protokół z oględzin z dnia 8 grudnia 2017 r.

wsc-wszyscy@mazowieckie.pl, a kierownicy oddziałów zobowiązani są do uzyskania od pracowników potwierdzenia o zapoznaniu się z ogłoszonymi zmianami.

Podczas oględzin zweryfikowano zabezpieczenia budynku oraz 9 losowo wybranych stanowisk dostępowych uniemożliwiające dostęp osób nieuprawnionych do przetwarzania danych osobowych i wykorzystywania danych z KZR niezgodnie z celem ich uzyskania.

I. Zabezpieczenia organizacyjne.

1. Serwerownia – miejsce do którego podłączona jest końcówka systemu teleinformatycznego Pobyt v. 2

   W pomieszczeniu w którym zlokalizowana jest serwerownia prowadzony jest remont generalny[8]. Pomieszczenie docelowo ma zostać wyposażone w końcówkę Systemu Kontroli Dostępu (dalej SKD) WSC, System Sygnalizacji Włamania i Napadu (dalej SSWiN), system sygnalizacji przeciwpożarowej (dalej ppoż.). Klucz do pomieszczenia serwerowni przechowywany jest na stanowisku ochrony fizycznej realizowanej przez koncesjonowaną firmę ochrony osób i mienia RR SECURITY sp. z o.o. Klucz wydawany jest osobom uprawnionym.

   Nie jest prowadzona książka osób, które uzyskują dostęp do pomieszczenia serwerowni.

2. Wybrane przez zespół kontrolny pomieszczenia zajmowane przez pracowników WSC MUW, w których znajdują się stanowiska dostępowe do systemu teleinformatycznego Pobyt v. 2.

   Pomieszczenia nr: 301, 302, 317, 326 znajdują się na III piętrze budynku WSC MUW. Klucze do tych pomieszczeń przechowywane są na stanowisku ochrony fizycznej. Wydawane są przez służbę ochrony na podstawie karty magnetycznej pracownika i weryfikacji danych pracownika znajdujących się na karcie, które wyświetlane są na monitorze służby ochrony. Potwierdzenie pobrania jak też zwrócenia kluczy odbywa się po dodatkowym wczytaniu mikrochipu zintegrowanego z kluczem.

   a) dostęp do windy oraz korytarzy na których zlokalizowane są okazane pomieszczenia możliwy jest przez wczytanie karty mikroprocesorowej pracownika. Na korytarzach znajdują się centralki alarmowe za pomocą których możliwe jest uruchomienie jak również włączenie przez służbę ochrony SSWiN. Według ustnego oświadczenia dowódcy zmiany obecnie, ze względu na prowadzone prace remontowe system nie jest w pełni sprawny.
   b) na korytarzach znajdują się przyciski alarmowe sygnalizacji ppoż. Czujki systemu ppoż. Znajdują się we wszystkich okazanych pomieszczeniach III piętra.
   c) na korytarzach znajdują się kamery SMW, z których obraz przekazywany jest na stanowisko monitoringu wizyjnego zlokalizowane na I piętrze budynku. Służba w tym pomieszczeniu pełniona jest całodobowo. Obraz z kamer jest rejestrowany.
   d) we wszystkich okazanych pomieszczeniach znajdują się rolety okienne.

[8] prace remontowe planowo zakończone zostaną do końca br.

3. Pomieszczenia nr 14, 16 i 17, zlokalizowane na parterze budynku, w których prowadzona jest bieżąca obsługa interesantów i w których znajdują się wybrane przez zespół kontrolny stanowiska dostępowe do systemu teleinformatycznego Pobyt v. 2.
   a) dostęp do tych pomieszczeń jest możliwy za pomocą kart mikroprocesorowych pracowników. Jednakże ze względu na stałą obsługę interesantów system ten jest wyłączony w godzinach urzędowania. Interesanci są obsługiwani za pomocą systemu kolejkowego z przywołaniem w tzw. openspace. Monitory komputerów są ustawione w sposób uniemożliwiający podgląd przez interesantów.
   b) na salach tych zlokalizowane są kamery SMW oraz czujki SSWiN. Funkcjonują także inne wspomagające systemy bezpieczeństwa.
   c) okna pomieszczeń wyposażone są w rolety.
   d) klucze do okazanych pomieszczeń są pobierane i zdawane na takich samych zasadach jak opisane w pkt. 2.
4. Użytkownicy stanowisk dostępowych wytypowanych przez zespół kontrolny okazali stosowne upoważnienia do przetwarzania danych osobowych wydane przez Wojewodę Mazowieckiego.

II. Zabezpieczenia techniczne.

W ramach sprawdzenia zabezpieczeń technicznych przeprowadzono oględziny pomieszczeń serwerowni oraz stanowisk komputerowych użytkowników. Przeprowadzono weryfikację wersji (dat) definicji oprogramowania antywirusowego, weryfikację konfiguracji systemów operacyjnych, w tym ustawienie blokowania ekranu po bezczynności, zainstalowanego oprogramowania, głównie przeglądarek WWW służących do obsługi KZR oraz antywirusowego, a także czy z komputerów klienckich nie ma dostępu do sieci Internet. Sprawdzono czy użytkownicy w systemach operacyjnych nie posiadają administracyjnych uprawnień, a także czy konta użytkowników są zabezpieczone indywidualnymi hasłami, spełniającymi określone kryteria. Przeprowadzono rozmowy z użytkownikami końcowymi KZR oraz z administratorem sieci.

1. Pomieszczenia serwerowni.

Stwierdzono brak redundancji w systemie klimatyzacji, a także brak jasnej informacji dotyczącej czasu podtrzymania przez urządzenia UPS oraz systemu powiadamiania o zbyt wysokiej temperaturze.

2. Infrastruktura teleinformatyczna.

Ustalono, że brak jest agregatu prądotwórczego i/lub zasilaczy UPS zapewniających odpowiedni czas podtrzymania w przypadku zaniku zasilania – dotyczy elementów infrastruktury (m.in. urządzeń sieciowych) jak i komputerów klienckich.

3. Komputery użytkowników.

Kontrola wykazała, iż na stanowiskach dostępowych do systemu teleinformatycznego Pobyt v.2 znajdowały się nieaktualne definicje antywirusowe, a w jednym ze sprawdzanych komputerów brak było oprogramowania antywirusowego. We wszystkich przypadkach ekran nie blokował się w czasie bezczynności. Brak było aktualizacji do systemu operacyjnego, a w dwóch

przypadkach stwierdzono niewspierany system operacyjny[9]. Odnotowano nieaktualne wersje przeglądarek WWW.

W odpowiedzi na wyniki oględzin kontrolowany podmiot przekazał[10] dodatkowe wyjaśnienia dotyczące kwestii technicznych, poinformował o podjęciu natychmiastowych działań, które wyeliminowały stwierdzone nieprawidłowości dotyczące aktualizacji oprogramowania i ustawień stanowisk komputerowych. Jeśli zaś chodzi o kwestie sprzętowe to zespół kontrolny otrzymał informację, że *(...) wymiana wszystkich niewspieranych systemów operacyjnych wraz z komputerami jest przewidziana w jednym z zadań projektu FAMI (...), do realizacji w pierwszej połowie 2018 roku (...)*, oraz, że *(...) z końcem 2017 roku pomieszczenie serwerowni (...) będzie posiadało redundantny system klimatyzacji, a w przyszłorocznym budżecie zaplanowano środki na modernizację systemu zasilania awaryjnego tego pomieszczenia.*

Biorąc pod uwagę fakt, iż część ze wskazanych przez zespół kontrolny nieprawidłowości zostało usuniętych natychmiast, a pozostała część zostanie wyeliminowana w najbliższym czasie realizacja przez Wojewodę Mazowieckiego, warunków określonych w art. 453 ustawy, umożliwiających udostępnianie danych przetwarzanych w krajowym zbiorze rejestrów, ewidencji i wykazu w sprawach cudzoziemców za pomocą urządzeń telekomunikacyjnych, a w szczególności spełnianie przez Wojewodę Mazowieckiego warunków określonych w art. 453 ust. 1 i 2 ustawy należy ocenić **pozytywnie z nieprawidłowościami.**

III. Zalecenia i wnioski pokontrolne.

1. Zapewnić rozliczalność osób uzyskujących fizyczny dostęp do pomieszczeń serwerowni poprzez objęcie ich SKD, odnotowywanie faktów pobrania kluczy oraz stosowanie książek ewidencyjnych (w przypadku braku możliwości objęcia ich SKD).
2. Zastosować system monitoringu wizyjnego w pomieszczeniach serwerowni.
3. Zastosować system dodatkowych klimatyzatorów w pomieszczeniach serwerowni, działających naprzemiennie w celu zapewnienia redundancji.
4. Kontynuować bieżącą aktualizację definicji antywirusowych na wszystkich komputerach oraz bieżące monitorowanie systemu ich automatycznej aktualizacji.
5. Na bieżąco przeprowadzać aktualizację wersji przeglądarek WWW na komputerach klienckich;
6. Zaktualizować systemy operacyjne na komputerach klienckich oraz na bieżąco utrzymywać ich aktualny stan.
7. Wycofać niewspierane systemy operacyjne i oprogramowanie z komputerów klienckich.
8. Wdrożyć system agregatu prądotwórczego i/lub zasilaczy UPS w celu zapewnienia poprawnego działania infrastruktury w przypadku zaniku zasilania.

Proszę o poinformowanie mnie o sposobie realizacji zaleceń wymienionych w **pkt 1-6** w terminie **do 31 stycznia 2018r.**, natomiast zaleceń wskazanych w **pkt 7-8** w terminie **do 30 września 2018r.**

[9] zainstalowana jest niewspierana od 2014 r. wersja systemu Windows XP
[10] pismo nr WSC-VI.1234.72.2017 z dnia 14 grudnia 2017 r.

Protokół sporządzono w dwóch jednobrzmiących egzemplarzach po jednym dla każdej ze stron.

*

* *

Zgodnie z § 10 ust. 2 rozporządzenia Ministra Spraw Wewnętrznych z dnia 28 kwietnia 2014 r. *w sprawie kontroli korzystania z dostępu do danych przetwarzanych w krajowym zbiorze rejestrów, ewidencji i wykazu w sprawach cudzoziemców za pomocą urządzeń telekomunikacyjnych lub systemów teleinformatycznych,* kierownik podmiotu kontrolowanego może wnieść do protokołu kontroli umotywowane pisemne zastrzeżenia w terminie 7 dni licząc od dnia otrzymania protokołu kontroli.

Zgodnie z § 12 ust. 1 rozporządzenia, kierownik podmiotu kontrolowanego może odmówić podpisania protokołu kontroli i składa Szefowi Urzędu pisemne wyjaśnienie tej odmowy w terminie 7 dni roboczych od dnia otrzymania protokołu kontroli.

NACZELNIK
WYDZIAŁU KONTROLI I NADZORU
BIURA SZEFA URZĘDU
Urzędu do Spraw Cudzoziemców
.....

ADMINISTRATOR
BEZPIECZEŃSTWA INFORMACJI
Urzędu do Spraw Cudzoziemców
Dariusz KROCZKOWSKI
.....

WOJEWODA MAZOWIECKI

.....
Zdzisław Sipiera
(pieczątka imienna i podpis kierownika podmiotu kontrolowanego)

M. Gorlicki
.....
(podpisy kontrolujących)

W przypadku odmowy podpisania protokołu – wzmianka o tym fakcie:

.....

.....

.....