SZEF URZĘDU DO SPRAW
CUDZOZIEMCÓW

RPW/173650/2019 P
Data:2019-12-18

Warszawa, dn. 27.11.2019 r.

BSZ.WKiN.091.2.2019/BK

PROTOKÓŁ KONTROLI

Na podstawie art. 455 ust. 1 ustawy z dnia 12 grudnia 2013 r. *o cudzoziemcach* (t.j. Dz. U. z 2018 r. poz. 2094 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) oraz zapisami *Polityki Bezpieczeństwa Krajowego Systemu Informatycznego (KSI) Centralnego Organu Technicznego dla Organów i Służb poziom wysoki wersja 2.0* kontrolę w Wydziale Spraw Obywatelskich i Cudzoziemców Warmińsko-Mazurskiego Urzędu Wojewódzkiego[1] położonego przy Al. Marszałka Józefa Piłsudskiego 7/9 w Olsztynie przeprowadził zespół kontrolny w składzie:

- **Bartosz Koneczny**, Naczelnik Wydziału Kontroli i Nadzoru w Biurze Szefa Urzędu, upoważnienie nr 10/2019 – kierownik zespołu kontrolnego,
- **Dariusz Mroczkowski**, Inspektor Ochrony Danych w Urzędzie do Spraw Cudzoziemców, upoważnienie nr 11/2019 – członek zespołu kontrolnego,
- [redacted] podreferendarz w Biurze Informatyki Urzędu do Spraw Cudzoziemców, upoważnienie nr 16/2019 – członek zespołu kontrolnego.

Kierownikiem podmiotu kontrolowanego w okresie poddanym kontroli był Wojewoda Warmińsko-Mazurski Pan Artur Chojecki. Jako osobę do kontaktu z zespołem kontrolnym wyznaczono Kierownika Oddziału w WSOiC W-M UW [redacted].

Przedmiotem kontroli była realizacja przez uprawniony podmiot wskazany w art. 450 ust. 1 pkt. 1 ustawy o cudzoziemcach, jakim jest Wojewoda Warmińsko-Mazurski, warunków określonych w art. 453 ustawy, umożliwiających udostępnianie danych przetwarzanych w krajowym zbiorze rejestrów, ewidencji i wykazu w sprawach cudzoziemców[3] za pomocą urządzeń telekomunikacyjnych, a w szczególności spełnianie przez Wojewodę Warmińsko-Mazurskiego warunków określonych

---

[1] dalej WSOiC W-M UW
[2] upoważnienie z dnia 16.10.2019 r
[3] dalej KZR

Wpłynęło dnia
2019 -12- 17
Urząd do Spraw Cudzoziemców

w art. 453 ust. 1 i 2 ustawy oraz realizacja przez Wojewodę Warmińsko-Mazurskiego przepisów rozporządzeń Ministra Spraw Wewnętrznych i Administracji w tym zakresie oraz *Polityki Bezpieczeństwa Krajowego Systemu Informatycznego (KSI)*[4] *Centralnego Organu Technicznego dla Organów i Służb poziom wysoki wersja 2.0*. Kontrolowany okres to 1stycznia do 31 lipca 2019 r.

Podczas oceny[5] spełniania przez kontrolowany podmiot warunków określonych w art. 453 ust. 1 i 2 ustawy zespół kontrolny weźmie pod uwagę następujące kategorie:

1. Stosowane zabezpieczenia urządzeń telekomunikacyjnych lub systemów teleinformatycznych przeznaczonych do komunikowania się z krajowym zbiorem rejestrów, ewidencji i wykazu w sprawach cudzoziemców;
2. 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.

Podczas oceny wykorzystywania przez Wojewodę Warmińsko-Mazurskiego danych poprzez KSI zespół kontrolny weźmie pod uwagę następujące kategorie:

1. Prowadzenie niezbędnej dokumentacji tzn. ewidencji UK, posiadanie zaświadczeń o ukończeniu szkolenia z zakresu bezpieczeństwa i ochrony danych wykorzystywanych poprzez KSI, posiadanie przez UK ważnych upoważnień do przetwarzania danych osobowych wydanych przez podmiot kontrolowany;
2. Czy dostęp UK do danych wykorzystywanych poprzez KSI jest niezbędny ze względu na zadania wykonywane przez danego pracownika kontrolowanej jednostki.

Pismem z dnia 5 maja 2014 r. Wojewoda Warmińsko-Mazurski wystąpił do Szefa Urzędu do Spraw Cudzoziemców[6] z wnioskiem na podstawie art. 453 ustawy o cudzoziemcach o wyrażenie zgody na udostępnianie danych przetwarzanych w KZR za pomocą urządzeń telekomunikacyjnych. 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.

---

[4] dalej KSI
[5] zastosowano 4-stopniową skalę ocen pozytywna, pozytywna z uchybieniami, pozytywna z nieprawidłowościami, negatywna
[6] dalej UdSC

Decyzją z dnia 6 maja 2014 r. nr 7/2014 Szef Urzędu wyraził zgodę Wojewodzie Warmińsko-Mazurskiemu na udostępnianie danych przetwarzanych w KZR za pomocą urządzeń telekomunikacyjnych.

Według stanu na dzień 20 września 2019 r. w podmiocie podlegającym kontroli aktywne były 33 konta w systemie teleinformatycznym Pobyt v.2 za pośrednictwem którego użytkownicy indywidulani uzyskują dostęp do krajowego zbioru rejestrów, ewidencji i wykazu w sprawach cudzoziemców. Z informacji przekazanych przez BI wynika również, że 9 spośród użytkowników indywidualnych z W-M UW w okresie od 01.01. do 31.07.2019 r. nie logowało się do SI POBYT v.2.

Z wyjaśnień[7] przekazanych przez kontrolowaną jednostkę wynika, iż w 6 przypadkach użytkownicy nadal są pracownikami WSOiC W-M UW, a brak logowania do systemu wynika z przyczyn obiektywnych. Jak wskazano w 3 przypadkach fakt konieczności cofnięcia uprawnień nie został zgłoszony ze względu na natłok pracy. Wyjaśniono również, że z takim wnioskiem wystąpiono w dniu 27 września 2019 r.

Według stanu na dzień 20 września 2019 r. pracownikom kontrolowanego podmiotu wydano 11 upoważnień dla użytkowników końcowych KSI. Z danych z BI wynika, że w 3 przypadkach konta zostały zamknięte, jeden z użytkowników ostatni raz logował się do SI POBYT w 2010 r., natomiast jedna z osób posiada obecnie dostęp z ramienia PSG Olsztyn. Wojewoda Warmińsko-Mazurski nie powiadomił Szefa UdSC o konieczności unieważnienia upoważnień do dostępu do danych KSI.

W cytowanym wyżej piśmie wyjaśniono, że *(...) występując do Szefa Urzędu do Spraw Cudzoziemców z wnioskami o cofnięcie dostępu do systemu informatycznego POBYT v.2 ww. użytkownikom traktowaliśmy to jako jednoznacznie z usunięciem ww. osobom upoważnień do przetwarzania danych w KSI (...).*

W tym miejscu należy zaznaczyć, iż pismem z dnia 24 października br. Wojewoda Warmińsko-Mazurski wystąpił o unieważnienie upoważnień do przetwarzania danych KSI przez osoby, które nie są już pracownikami WSOiC W-M UW[8].

W czasie kontroli ustalono, iż wszyscy użytkownicy końcowi posiadali ważne upoważnienia do przetwarzania danych osobowych wydanych przez podmiot kontrolowany oraz, że dostęp użytkowników do danych wykorzystywanych poprzez KSI jest niezbędny ze względu na zadania wykonywane przez danego pracownika kontrolowanej jednostki. Z wyjaśnień kontrolowanej jednostki wynika, że *(...) wgląd danych lub wpis danych (...) następują w związku z prowadzonymi postępowaniami administracyjnymi. Pracownicy w zadekretowanych na siebie sprawach dokonują odpowiednich sprawdzeń i/lub wpisów i nanoszą we wnioskach odpowiednie adnotacje. Kontrola i nadzór nad pracownikami wynika bezpośrednio z kodeksu pracy, jak i zakresów czynności kierownika oddziału oraz Dyrektora Wydziału (...).*

Osoby uzyskujące dostęp do KZR oraz do danych przetwarzanych w KSI zapoznały się z *Instrukcja Zarządzania Systemem Teleinformatycznym Pobyt v.2, wersja 8.0 WBIOIN.270.2.2018/DM*

---

[7] pismo SO-X.1610.1.2019 z dnia 01.10.2019 r.
[8] pismo SO-X 6156.1.93.2019 AW z dnia 24.10.2019 r.

z dnia 2 lipca 2018 r. oraz *Polityką Bezpieczeństwa Krajowego Systemu Informatycznego (KSI) Centralnego Organu Technicznego dla Organów i Służb poziom wysoki wersja 2.0.* Dokumenty te zostały udostępnione pracownikom poprzez system EZD PUW, dodatkowo dokumentacja ta umieszczona jest na wydzielonym w tym celu dysku, do którego dostęp ze swojego komputera ma każdy pracownik WSOiC W-M UW. Z przekazanych za pismem z dnia 1 października 2019 r. wyjaśnień wynika, że w kontrolowany *(…) organ dotychczas nie prowadził odrębnej ewidencji osób które zapoznały się z Instrukcją (…)* czy *(…) Polityką Bezpieczeństwa (…).* W tym miejscu należy podkreślić, iż zgodnie z punktem 1.1 pkt. 6 cytowanej wyżej *Polityki Bezpieczeństwa (…)* każdy organ prowadzi własną dokumentację opisującą sposób przetwarzania danych KSI oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych objętych ochroną zawierającą min. oświadczenia o zapoznaniu się użytkownika KSI z polityką bezpieczeństwa.

Pismem z dnia 24 października 2019 r.[9] poinformowano, iż *(…) w związku z ustaleniami poczynionymi podczas oględzin mających miejsce w tut. urzędzie 17-18.10.2019 r., pracownicy Wydziału Spraw Obywatelskich i Cudzoziemców mający dostęp do systemów KSI i Pobyt v.2 potwierdzili zapoznanie się z „Polityką Bezpieczeństwa Krajowego Systemu Informatycznego (KSI) Centralnego Organu Technicznego dla Organów i Służb poziom wysoki wersja 2.0." oraz „Instrukcją Zarządzania Systemem Teleinformatycznym POBYT v.2 wer. 8.0", składając podpis na aktualnych dokumentach (…).*

Zespołowi kontrolnemu przedstawiono dokumentację dotyczącą szkoleń z zakresu bezpieczeństwa i ochrony danych wykorzystywanych poprzez KSI. Użytkownicy końcowi KSI w W-M UW przeszkoleni zostali przez wykwalifikowanych trenerów, otrzymali zaświadczenia potwierdzające odbycie szkolenia i złożyli oświadczenia o odbyciu szkolenia. Należy jednak zaznaczyć, iż żaden z przedstawionych zespołowi kontrolnemu *Planów Szkolenia* nie był w pełni zgodny z przepisami rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 6 maja 2008 r. *w sprawie sposobu przeprowadzania szkoleń z zakresu bezpieczeństwa i ochrony danych wykorzystywanych przez Krajowy System Informatyczny oraz kwalifikacji osób uprawnionych do przeprowadzenia szkoleń (Dz. U. z 2008 r. nr 80 poz. 482)* zgodnie z którymi *Plan szkolenia* opracować ma administrator bezpieczeństwa informacji uprawnionego organu (obecnie Inspektor Ochrony Danych), a zatwierdzić kierownik uprawnionego organu, czyli w tym przypadku Wojewoda Warmińsko-Mazurski.

Powyższe należy potraktować jako **uchybienie**.

W toku kontroli ustalono, że w Warmińsko-Mazurskim Urzędzie Wojewódzkim w Olsztynie nie opracowano i nie wdrożono procedur kontrolnych, o których mowa w punkcie 1.6 *Polityki Bezpieczeństwa Krajowego Systemu Informatycznego (KSI) Centralnego Organu Technicznego dla Organów i Służb poziom wysoki wersja 2.0.*

Powyższe należy uznać za **uchybienie**.

---

[9] pismo SO-X 1610 1.2019 z dnia 24 10 2019 r.

W toku kontroli zespół kontrolny dokonał oględzin w siedzibie WSOiC W-M UW w której zlokalizowane są stanowiska dostępowe do KZR i KSI[10]. Podczas oględzin zweryfikowano zabezpieczenia budynku serwerowni oraz stanowisk dostępowych uniemożliwiające dostęp osób nieuprawnionych do przetwarzania danych osobowych i wykorzystywania danych z KZR i KSI niezgodnie z celem ich uzyskania.

I. Zabezpieczenia organizacyjne.

Zespół kontrolny nie miał zastrzeżeń co do zastosowanych zabezpieczeń organizacyjnych serwerowni oraz znajdujących się na parterze budynku W-M UW pomieszczeń w których zlokalizowane są stanowiska komputerowe z których możliwy jest dostęp do KZR oraz KSI.

II. Zabezpieczenia techniczne.

W ramach sprawdzenia zabezpieczeń technicznych przeprowadzono oględziny pomieszczeń serwerowni oraz stanowisk komputerowych użytkowników.
Przeprowadzono weryfikację oprogramowania antywirusowego, weryfikację wersji systemów operacyjnych i zainstalowanych aktualizacji, 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 (długość min. 8 znaków, małe i wielkie litery, znaki specjalne). Przeprowadzono rozmowy z użytkownikami końcowymi KZR oraz z administratorem sieci.

1. Pomieszczenia serwerowni.

   Brak uwag.

2. Komputery użytkowników.

Kontrola wykazała, iż na stanowiskach dostępowych do systemu teleinformatycznego Pobyt v.2 oraz do danych przetwarzanych w KSI brak jest oprogramowania antywirusowego oraz nieaktualność definicji wbudowanego oprogramowania antywirusowego, a w jednym ze sprawdzanych komputerów brak było oprogramowania antywirusowego. Stwierdzono, że użytkownicy mają możliwość wyłączenia funkcji blokowania ekranu po bezczynności. W Polityce Ochrony Danych w Warmińsko-Mazurskim Urzędzie Wojewódzkim[11] oraz w Zasadach Bezpieczeństwa Danych Osobowych w Oddziale Legalizacji Pobytu Cudzoziemców znajdują się wprawdzie zapisy dotyczące tzw. polityki haseł, jednak ustawienia stanowisk nie wymuszały okresowej zmiany haseł, brak też było wymuszania aby hasła spełniały warunki określone w tych dokumentach. Brak było aktualizacji do

---

[10] protokół z oględzin z dnia 18.10.2019 r.

[11] Załącznik nr 1 do Zarządzenia nr 128 Wojewody Warmińsko-Mazurskiego dnia 24.05.2018 r.

systemu operacyjnego, a w dwóch przypadkach stwierdzono niewspierany system operacyjny[12]. Odnotowano także nieaktualne wersje przeglądarek WWW. Brak było blokady podłączania nośników danych, co może prowadzić do niekontrolowanego ich podłączania. Stwierdzono również fakt używania jednego konta użytkownika dla wielu osób do logowania się do systemu operacyjnego.

Powyższe należy potraktować jako **nieprawidłowości**, za które odpowiedzialność ponosi administrator systemów informatycznych W-M UW.

Biorąc pod uwagę powyższe należy ocenić **pozytywnie z nieprawidłowościami** realizację przez Wojewodę Warmińsko-Mazurskiego, warunków określonych w art. 453 ust. 1 i 2 ustawy o cudzoziemcach, umożliwiających udostępnianie danych przetwarzanych w krajowym zbiorze rejestrów, ewidencji i wykazu w sprawach cudzoziemców za pomocą urządzeń telekomunikacyjnych oraz przepisów związanych z wykorzystywaniem danych przetwarzanych przez Krajowy System Informatyczny.

III. Zalecenia i wnioski pokontrolne.

1. Przygotowywane programy szkolenia z zakresu bezpieczeństwa i ochrony danych wykorzystywanych przez KSI powinny być w pełni zgodne z przepisami rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 6 maja 2008 r. *w sprawie sposobu przeprowadzania szkoleń z zakresu bezpieczeństwa i ochrony danych wykorzystywanych przez Krajowy System Informatyczny oraz kwalifikacji osób uprawnionych do przeprowadzenia szkoleń (Dz. U. z 2008 r. nr 80 poz. 482);*
2. Należy opracować i wdrożyć procedurę kontroli wykorzystania danych KSI oraz przekazać informację o tym fakcie do Centralnego Organu Technicznego KSI;
3. Należy zainstalować (lub używać wbudowanego) i na bieżąco aktualizować oprogramowanie chroniące przed złośliwym oprogramowaniem;
4. Należy zaktualizować systemy operacyjne oraz utrzymywać ich aktualny stan na bieżąco;
5. Należy zablokować możliwość wyłączenia przez użytkowników blokowania ekranów po bezczynności;
6. Należy wycofać z użytkowania niewspierane systemy operacyjne i oprogramowanie;
7. Należy wdrożyć mechanizm wymuszania okresowej zmiany haseł oraz mechanizm wymuszania silnych i niepowtarzających się haseł;
8. Należy stosować indywidualne konta dla wszystkich użytkowników;
9. Należy niezwłocznie odebrać użytkownikom uprawnienia administracyjne;
10. Należy rozważyć kontrolowanie użycia nośników danych.

Jednocześnie informuję, że w przypadku wątpliwości co do technicznych możliwości przeprowadzenia aktualizacji systemów operacyjnych lub oprogramowania chroniącego przed złośliwym oprogramowaniem wsparcie można uzyskać pisząc na adres: [redacted]

---

[12] zainstalowana jest niewspierana od 2014 r. wersja systemu Windows XP

Pismem z dnia 15 listopada 2019 r. sygn. SO-X.1610.1.2019 kierownik kontrolowanej jednostki wniósł zastrzeżenie do protokołu w kwestii stwierdzonego przez zespół kontrolny uchybienia dotyczącego formy *planu szkolenia z zakresu bezpieczeństwa i ochrony danych SIS i danych VIS*.

Biorąc pod uwagę fakt, że jak wykazano w stanowisku Szefa Urzędu do Spraw Cudzoziemców do zastrzeżeń, [redacted] nie posiadała upoważnienia do zatwierdzenia *planów szkoleń z zakresu bezpieczeństwa i ochrony danych SIS i danych VIS* stwierdzono, że żaden z przedstawionych zespołowi kontrolnemu planów nie spełnia warunków określonych w przepisach rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 6 maja 2008 r. *w sprawie sposobu przeprowadzania szkoleń z zakresu bezpieczeństwa i ochrony danych wykorzystywanych przez Krajowy System Informatyczny oraz kwalifikacji osób uprawnionych do przeprowadzenia szkoleń (Dz. U. z 2008 r. nr 80 poz. 482)*.

Dlatego też, zgodnie z § 11 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) zastrzeżenie zostało oddalone w całości.

Proszę o poinformowanie mnie o sposobie realizacji zaleceń pokontrolnych w terminie <u>do dnia 31 grudnia 2019 r.</u>

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

*

* *

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

Inspektor Ochrony Danych
Urząd do Spraw Cudzoziemców
Dariusz Mroczkowski
....

[redacted]
....

(podpisy kontrolujących)

WOJEWODA
WARMIŃSKO-MAZURSKI
..................Artur Chojecki

(pieczątka imienna i podpis kierownika podmiotu kontrolowanego)

W przypadku odmowy podpisania protokołu – wzmianka o tym fakcie:

……

……

……