SZEF URZĘDU DO SPRAW CUDZOZIEMCÓW

RPW/97083/2025_P
Data:2025-04-07

Ł- wa, dn. 28.03.20

ŁÓDZKI URZĄD WOJEWÓDZKI W ŁODZI
KANCELARIA GŁÓWNA URZĘDU
Data wpływu: 2025 -04- 07
2
UL. PIOTRKOWSKA 104 90-926 ŁÓDŹ
dziennika .....

BSZ.WKiN.091.2.2024/HT

Pani
Dorota Ryl
WOJEWODA ŁÓDZKI

Szanowna Pani Wojewodo,

w załączeniu przekazuję dwa egzemplarze protokołu z kontroli przeprowadzonej na podstawie art. 453 ustawy o cudzoziemcach /t.j. Dz. U. z 2024 r., poz. 769 z późn. zm/, umożliwiających udostępnianie danych przetwarzanych w krajowym zbiorze rejestrów, ewidencji i wykazu w sprawach cudzoziemców za pomocą urządzeń telekomunikacyjnych oraz wykorzystywania danych z Krajowego Systemu Informatycznego (KSI) przez pracowników Łódzkiego Urzędu Wojewódzkiego – z prośbą o ich podpisanie i zwrot jednego z egzemplarzy.

Zgodnie z § 10 ust. 1 i 2 *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 (KZR) za pomocą urządzeń telekomunikacyjnych lub systemów teleinformatycznych /Dz.U. z 2014 r., poz. 551/*, kierownik podmiotu kontrolowanego może wnieść do protokołu kontroli umotywowane pisemne zastrzeżenia w terminie 7 dni licząc od dnia otrzymania protokołu kontroli.

Jednocześnie informuję, że zgodnie z § 12 ust. 1 cyt. wyżej rozporządzenia, kierownik podmiotu kontrolowanego może odmówić podpisania protokołu kontroli i złożyć Szefowi Urzędu pisemne wyjaśnienie tej odmowy w terminie 7 dni roboczych od dnia otrzymania protokołu kontroli.

Podpisany protokół bądź wniesione zastrzeżenia należy przekazać na adres do korespondencji Urzędu do Spraw Cudzoziemców: ul. Taborowa 33, 02-699 Warszawa.

SZEF
Urzędu do Spraw Cudzoziemców
Tomasz Cytrynowicz

Załączniki:

1. Protokół kontroli z 24.03.2025 r.

SZEF URZĘDU DO SPRAW CUDZOZIEMCÓW

Warszawa, 24 marca 2025 r.

BSZ.WKIN.091.2.2024/KK

PROTOKÓŁ KONTROLI

Na podstawie art. 455 ust. 1 ustawy z dnia 12 grudnia 2013 r. o cudzoziemcach /t.j. Dz. U. z 2024 r., poz. 769 z późn. zm. – dalej: ustawa o cudzoziemcach/ 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 (KZR) za pomocą urządzeń telekomunikacyjnych lub systemów informatycznych* /Dz. U. z 2014 r., poz. 551/, zespół kontrolny w składzie:

- Piotr Piechowiak – główny specjalista w Wydziale Kontroli i Nadzoru Biura Szefa Urzędu do Spraw Cudzoziemców, kierownik zespołu kontrolnego[1],
- Krystyna Komorniak – naczelnik Wydziału Kontroli i Nadzoru Biura Szefa Urzędu do Spraw Cudzoziemców, członek zespołu kontrolnego,
- Marek Goślicki – informatyk w Biurze Informatyki Urzędu do Spraw Cudzoziemców, członek zespołu kontrolnego,

przeprowadził kontrolę w Wydziale Spraw Cudzoziemców Łódzkiego Urzędu Wojewódzkiego w Łodzi, położonym przy ul. Piotrkowskiej 103 w Łodzi.

Kierownikiem podmiotu kontrolowanego w okresie poddanym kontroli był Wojewoda Łódzki – Pani Dorota Ryl.

Przedmiotem kontroli była realizacja przez uprawniony podmiot wskazany w art. 450 ust. 1 pkt 1 ustawy o cudzoziemcach, jakim jest Wojewoda Łódzki, warunków określonych w art. 453 ustawy, umożliwiających udostępnianie danych przetwarzanych w krajowym zbiorze rejestrów, ewidencji i wykazu w sprawach cudzoziemców za pomocą urządzeń telekomunikacyjnych oraz wykorzystywania danych z Krajowego Systemu Informatycznego (KSI) przez pracowników Łódzkiego Urzędu Wojewódzkiego w Łodzi, a w szczególności spełnianie przez Wojewodę Łódzkiego warunków określonych w art. 453 ust. 1 i 2 ustawy oraz realizacja przez Wojewodę Łódzkiego przepisów rozporządzeń Ministra Spraw Wewnętrznych i Administracji w tym zakresie oraz Polityki Bezpieczeństwa Krajowego Systemu Informatycznego (KSI) Centralnego Organu Technicznego dla Organów i Służb poziom wysoki wersja 2.0. Kontrolowany okres to 01.01.2024 r. – 30.09.2024 r.

Podczas oceny spełniania przez kontrolowany podmiot warunków określonych w art. 453 ust. 1 i 2 ustawy o cudzoziemcach, zespół kontrolny wziął pod uwagę następujące kategorie:

[1] Z dniem 31.12.2024 r. za porozumieniem stron zmieniono formę zatrudnienia pana Piotra Piechowiaka z umowy o pracę na umowę zlecenie.

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

Pismem z dnia 02.05.2014 r. Wojewoda Łódzki wystąpił do Szefa Urzędu do Spraw Cudzoziemców (dalej: Szef Urzędu) z wnioskiem na podstawie art. 453 ustawy o cudzoziemcach o wyrażenie zgody na udostępnienie danych przetwarzanych w krajowym zbiorze rejestrów, ewidencji i wykazu w sprawach cudzoziemców za pomocą urządzeń telekomunikacyjnych. Organ wnioskujący oświadczył, że spełnia warunki wskazane w art. 453 ustawy o cudzoziemcach, tj.:

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

Decyzją z dnia 02.05.2014 r. nr 3/2014 Szef Urzędu na podstawie art. 454 ust. 1 ustawy o cudzoziemcach wyraził zgodę na udostępnienie Wojewodzie Łódzkiemu danych przetwarzanych w krajowym zbiorze rejestrów, ewidencji i wykazu w sprawach cudzoziemców za pomocą urządzeń telekomunikacyjnych.

Według stanu na dzień 12.11.2024 r. w podmiocie podlegającym kontroli aktywnych było 119 kont w systemie teleinformatycznym Pobyt v.3, za pośrednictwem którego użytkownicy indywidualni uzyskują dostęp do krajowego zbioru rejestrów, ewidencji i wykazu w sprawach cudzoziemców. Z informacji przekazanych przez Biuro Informatyki Urzędu do Spraw Cudzoziemców (dalej: Biuro Informatyki Urzędu) wynika również, że 3 użytkowników indywidualnych z Łódzkiego Urzędu Wojewódzkiego w Łodzi w okresie od 01.01.2024 r. do 30.09.2024 r. nie logowało się do systemu teleinformatycznego Pobyt.

Z wyjaśnień Pana Pawła Kowalczyka, Dyrektora Wydziału Spraw Cudzoziemców ŁUW, przedstawionych w piśmie z dnia 20.11.2024 r. nr: S.C.-II.6156.68.2024 r.[2], wynika, iż spośród trzech pracowników, którzy nie logowali się w systemie teleinformatycznym Pobyt, jeden pracownik, Pan [redacted] posiada uprawnienia do korzystania z systemu Pobyt dopiero od 07.10.2024 r. Pozostałe dwie osoby są pracownikami Wydziału Spraw Obywatelskich i realizują zadania w ramach postępowań o wydanie zezwolenia na pracę. Pani [redacted] przebywa na długotrwałym zwolnieniu lekarskim, a Pan [redacted] podczas oddelegowania do innego Oddziału korzystał z systemu Pobyt, jednak jego obecny zakres obowiązków nie obejmuje przetwarzania danych w KZR; jego uprawnienia zostały cofnięte. Dyrektor Biura Informatyki Urzędu do Spraw Cudzoziemców potwierdził fakt cofnięcia w dniu 19.11.2024 r. uprawnień panu Krzysztofowi Grausam.

Odnosząc się do kwestii szkoleniowych oraz dostępu do przetwarzania danych osobowych, Dyrektor Wydziału Spraw Cudzoziemców ŁUW wyjaśnił, iż każdy nowo zatrudniony pracownik jest przeszkolony w zakresie przetwarzania danych osobowych oraz posiada upoważnienia do dostępu i przetwarzaniach danych osobowych w ramach Łódzkiego Urzędu Wojewódzkiego w Łodzi. Wszystkie osoby uzyskujące dostęp do systemu Pobyt mają obowiązek zapoznania się z treścią Instrukcji Zarządzania Systemem Teleinformatycznym Pobyt nr DKBM.WBOIN.2703.84.2022/WW, który to obowiązek realizują. W Wydziale Spraw Cudzoziemców nie jest prowadzony wykaz osób, które powinny zapoznać się z ww. polityką.

[2] Dalej: pismo nr: S.C.-II.6156.68.2024 r.

Brak wykazu osób, które zapoznały się z aktualną Instrukcją Zarządzania Systemem Teleinformatycznym Pobyt uznano za uchybienie.

Podmiot kontrolowany poinformował zespół kontrolny[3], iż jednym z elementów szkoleń pracowników w zakresie użytkowania SIS i VIS, bezpieczeństwa i jakości danych, praw podstawowych oraz procedur regulujących przetwarzanie danych, jest omówienie polityki ochrony danych osobowych, przetwarzanych poprzez KSI dla organów i służb, której treść jest udostępniona przez Komendanta Głównego Policji. Szkolenia prowadzone są przez wyznaczonych i wykwalifikowanych instruktorów w Łódzkim Urzędzie Wojewódzkim w Łodzi. Jednostka kontrolowana przekazała wykaz osób, które odbyły stosowne szkolenie oraz zaświadczenia potwierdzające ukończenie kursu[4]. Przy tym poinformowano zespół kontrolny, iż pracownicy Wydziału Spraw Cudzoziemców nie korzystają z SIS i VIS z poziomu systemu Pobyt, tylko wykorzystują karty mikroprocesorowe oraz działającą niezależnie od SI Pobyt aplikację siswww, której administratorem jest Komendant Główny Policji.

Z uwagi na fakt, że podmiot kontrolowany nie korzysta z dostępu do KSI za pośrednictwem systemu informatycznego Pobyt, lecz poprzez odrębną aplikację, która nie jest administrowana przez Szefa Urzędu do Spraw Cudzoziemców, odstąpiono od kontroli w zakresie dostępu do KSI.

Ponadto z wyjaśnień złożonych przez Dyrektora Wydziału Spraw Cudzoziemców[5] wynika, że podmiot kontrolowany wprowadził techniczne i organizacyjne zabezpieczenia stanowisk dostępowych do KZR i KSI, mające na celu uniemożliwienie dostępu osobom nieuprawnionym do przetwarzania danych osobowych oraz wykorzystywania ich niezgodnie z celem ich uzyskania. Ponadto prowadzi wykaz pomieszczeń, z których realizowany jest dostęp do KZR za pośrednictwem systemu teleinformatycznego POBYT. Zespołowi kontrolnemu przekazano kopię tego dokumentu[6].

Zabezpieczenia techniczne

Jednym z zastosowanych zabezpieczeń jest kontrola fizycznego dostępu do pomieszczeń, w których znajdują się stanowiska dostępowe do KZR i KSI. Kontrola ta realizowana jest przez pracowników ochrony, którzy wydają klucze do tych pomieszczeń wyłącznie uprawnionym pracownikom Wydziału.

Dostęp do systemu Pobyt jest zabezpieczony poprzez indywidualne uwierzytelnienie użytkownika za pomocą loginu i hasła. System wymusza cykliczną zmianę hasła w regularnych odstępach czasu. Ponadto komputery z dostępem do KZR i KSI są podłączone wyłącznie do wewnętrznej sieci Urzędu, która jest odseparowana od sieci publicznej. Każda stacja robocza z dostępem do KZR i KSI jest objęta ochroną za pomocą zapory Windows Defender. Nadzór nad siecią oraz zabezpieczenie systemów teleinformatycznych sprawuje Biuro Administracji i Logistyki Łódzkiego Urzędu Wojewódzkiego w Łodzi.

Zabezpieczenia organizacyjne

Dostęp do danych zgromadzonych w KZR i KSI jest przyznawany wyłącznie pracownikom, których zakres obowiązków wymaga przetwarzania tych danych. Przyznanie dostępu do systemu Pobyt następuje na podstawie pisemnego upoważnienia wydanego przez Dyrektora Wydziału, uprawniającego do dostępu do krajowego zbioru rejestrów, ewidencji i wykazu w sprawach cudzoziemców oraz wykorzystywania danych zawartych w tym rejestrze.

*

* *

[3] Pismo nr: S.C.-II.6156.68.2024 r.

[4] Załącznik do pisma nr: S.C.-II.6156.68.2024 r. – lista użytkowników systemów SIS i VIS w Oddziale Cudzoziemców do Spraw Legalizacji Pobytu i Pracy Wydziału Spraw Cudzoziemców; lista użytkowników systemów SIS i VIS Oddziale Cudzoziemców do Spraw Legalizacji Pobytu Wydziału Spraw Cudzoziemców; lista użytkowników systemów SIS i VIS w Oddziale Spraw Obywatelskich Wydziału Spraw Obywatelskich.

[5] Pismo nr: S.C.-II.6156.68.2024.

[6] Załącznik do pisma nr: S.C.-II.6156.68.2024 r.

W toku kontroli zespół kontrolny dokonał oględzin w siedzibie Wydziału Spraw Cudzoziemców Łódzkiego Urzędu Wojewódzkiego w Łodzi, w której zlokalizowane są stanowiska dostępowe do KZR[7]. Podczas oględzin zweryfikowano wszystkie pomieszczenia, w których znajdują się stanowiska dostępowe pod kątem zabezpieczeń uniemożliwiające dostęp osób nieuprawnionych do przetwarzania danych osobowych i wykorzystywania danych z KZR i KSI niezgodnie z celem ich uzyskania. Ponieważ skrzydło budynku, w którym znajduje się serwerownia jest w trakcie remontu, zespół kontrolny nie miał dostępu do budynku serwerowni i nie przeprowadził stosownych oględzin. Przyjęto informacje dotyczące zabezpieczeń, przekazane ustnie przez Pana [redacted] z zespołu informatyków ŁUW.

Zabezpieczenia organizacyjne.

Zespół kontrolny nie miał zastrzeżeń co do zastosowanych zabezpieczeń organizacyjnych pomieszczeń ŁUW, w których zlokalizowane są stanowiska komputerowe, z których możliwy jest dostęp do KZR oraz KSI.

Zabezpieczenia techniczne.

W ramach sprawdzenia zabezpieczeń technicznych przeprowadzono oględziny sześciu stanowisk komputerowych użytkowników usytuowanych w różnych pomieszczeniach w siedzibie WSC ŁUW. Wyrywkową kontrolę uzasadniały ustne wyjaśnienia złożone przez Pana [redacted] informatyka WSC ŁUW, z których wynikało, że na każdym stanowisku zastosowane są takie same rozwiązania i zabezpieczenia, co potwierdziły oględziny.

W ramach oględzin 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. Przeprowadzono rozmowy z użytkownikami końcowymi KZR oraz z administratorem sieci.

Na podstawie oględzin wybranych stanowisk oraz wyjaśnień pana [redacted] ustalono, iż:

- wszyscy użytkownicy korzystają z jednego, lokalnego konta Windows (zainstalowany system operacyjny to Windows 10 – licencja przypisana jest sprzętowo do płyty głównej każdego komputera), wspólnego dla wszystkich użytkowników, takiego samego na każdym stanowisku, z ustalonym na stałe hasłem, takim samym na każdym komputerze,
- logowanie do systemu teleinformatycznego Pobyt odbywa się w sposób zindywidualizowany, poprzez wpisanie przez każdego uprawnionego użytkownika loginu (nr PESEL) oraz hasła,
- na stacjach umożliwiających użytkownikom dostęp do systemu teleinformatycznego Pobyt brak jest aktualnych definicji programu antywirusowego, jak również aktualizacje Windows nie są systematycznie instalowane,
- ekrany monitorów użytkowników nie blokują się samoczynnie po bezczynności, natomiast po 30 minutach bezczynności włącza się wygaszacz ekranu,
- po 30 minutach bezczynności wygasa sesja w systemie teleinformatycznym Pobyt i wymagane jest ponowne zalogowanie się do systemu,
- na stanowiskach z dostępem do KZR nie ma możliwości korzystania z Internetu,
- na żadnym ze sprawdzonych stanowisk użytkownik nie posiada uprawnień administratora.

W wyniku przeprowadzonej kontroli stwierdzono następujące nieprawidłowości w zakresie zabezpieczeń systemu teleinformatycznego Pobyt:

- brak wykazu osób, które zapoznały się Zarządzania Systemem Teleinformatycznym POBYT nr DKBM.WBOIN.2703.84.2022/WW,

[7] Protokół z oględzin z dnia 29.11.2024 r.

- brak aktualnych definicji oprogramowania antywirusowego na stanowiskach dostępowych,
- brak systematycznej instalacji aktualizacji systemu operacyjnego Windows,
- brak automatycznej blokady ekranów monitorów użytkowników po okresie bezczynności,
- korzystanie z jednego, lokalnego konta użytkownika systemu operacyjnego wspólnego dla wszystkich użytkowników, identycznego na każdym stanowisku, z ustalonym na stałe hasłem, takim samym na wszystkich komputerach.

Powyższe należy potraktować jako uchybienie, za które odpowiedzialność ponosi administrator systemów informatycznych Łódzkiego Urzędu Wojewódzkiego w Łodzi.

Brak indywidualizacji dostępu do systemu, a także niestosowanie odpowiednich zabezpieczeń, takich jak aktualizacje oprogramowania czy oprogramowanie antywirusowe, naraża system na potencjalne ataki z sieci, wirusy czy inne formy cyberzagrożeń. Dodatkowo, brak blokady ekranów po okresie bezczynności i wspólne konto użytkowników utrudniają kontrolowanie dostępu do danych, co może prowadzić do nieautoryzowanego dostępu i utraty poufności informacji. Uznać należy, że stwierdzone uchybienia, choć nie miały charakteru jednostkowego, wpływały na kontrolowaną działalność w ograniczonym zakresie, stwarzając jednakowoż ryzyko naruszenia zasad bezpieczeństwa informatycznego, w tym ochrony danych osobowych.

W związku z powyższym, należy ocenić pozytywnie z uchybieniami realizację przez Wojewodę Łódzkiego 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. Uchybienia te powinny zostać niezwłocznie usunięte.

Zalecenia i wnioski pokontrolne.

W związku ze stwierdzonymi w toku kontroli uchybieniami w zakresie zabezpieczeń systemu teleinformatycznego Pobyt, zaleca się podjęcie niezwłocznych działań w celu ich usunięcia oraz zapewnienia właściwego poziomu bezpieczeństwa systemów informatycznych. W szczególności należy:

1. **Założyć i prowadzić wykaz osób**, które zapoznały się z aktualną Instrukcją Zarządzania Systemem Teleinformatycznym Pobyt.
2. **Zainstalować i aktualizować na bieżąco oprogramowanie antywirusowe** na wszystkich stanowiskach dostępowych do systemu teleinformatycznego Pobyt.
3. **Wprowadzić systematyczną instalację aktualizacji systemu operacyjnego Windows**, zapewniając jego bieżącą ochronę przed zagrożeniami.
4. **Skonfigurować automatyczną blokadę ekranów monitorów użytkowników** po określonym czasie bezczynności, aby zapobiec nieautoryzowanemu dostępowi.
5. **Zlikwidować praktykę korzystania z jednego, lokalnego konta Windows wspólnego dla wszystkich użytkowników** i wdrożyć indywidualne konta użytkowników z unikalnymi, okresowo zmienianymi silnymi hasłami.
6. **Zapewnić zgodność polityki bezpieczeństwa systemów informatycznych z obowiązującymi przepisami oraz dobrymi praktykami w zakresie ochrony danych i dostępu do systemów.**

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: biuroinformatyki@udsc.gov.pl.

Proszę o poinformowanie mnie o sposobie realizacji zaleceń pokontrolnych w terminie do dnia 25.04.2025 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 pisemnie 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.

.....
podpis kierownika zespołu kontrolnego

NACZELNIK
WYDZIAŁU KONTROLI I NADZORU
Biuro Szefa Urzędu
Urząd do Spraw Cudzoziemców

.....
podpis członka zespołu kontrolnego

.....
pieczątka imienna i podpis kierownika podmiotu kontrolowanego

M. Gaślicki
.....
podpis członka zespołu kontrolnego

W przypadku odmowy podpisania protokołu – wzmianka o tym fakcie:

.....

.....

.....

.....

.....

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.

SZEF URZĘDU DO SPRAW CUDZOZIEMCÓW

Warszawa, 24 marca 2025 r.

BSZ.WKiN.091.2.2024/KK

PROTOKÓŁ KONTROLI

Na podstawie art. 455 ust. 1 ustawy z dnia 12 grudnia 2013 r. o cudzoziemcach /t.j. Dz. U. z 2024 r., poz. 769 z późn. zm. – dalej: ustawa o cudzoziemcach/ 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 (KZR) za pomocą urządzeń telekomunikacyjnych lub systemów informatycznych* /Dz. U. z 2014 r., poz. 551/, zespół kontrolny w składzie:

- Piotr Piechowiak – główny specjalista w Wydziale Kontroli i Nadzoru Biura Szefa Urzędu do Spraw Cudzoziemców, kierownik zespołu kontrolnego[1],
- Krystyna Komorniak – naczelnik Wydziału Kontroli i Nadzoru Biura Szefa Urzędu do Spraw Cudzoziemców, członek zespołu kontrolnego,
- Marek Goślicki – informatyk w Biurze Informatyki Urzędu do Spraw Cudzoziemców, członek zespołu kontrolnego,

przeprowadził kontrolę w Wydziale Spraw Cudzoziemców Łódzkiego Urzędu Wojewódzkiego w Łodzi, położonym przy ul. Piotrkowskiej 103 w Łodzi.

Kierownikiem podmiotu kontrolowanego w okresie poddanym kontroli był Wojewoda Łódzki – Pani Dorota Ryl.

Przedmiotem kontroli była realizacja przez uprawniony podmiot wskazany w art. 450 ust. 1 pkt 1 ustawy o cudzoziemcach, jakim jest Wojewoda Łódzki, warunków określonych w art. 453 ustawy, umożliwiających udostępnianie danych przetwarzanych w krajowym zbiorze rejestrów, ewidencji i wykazu w sprawach cudzoziemców za pomocą urządzeń telekomunikacyjnych oraz wykorzystywania danych z Krajowego Systemu Informatycznego (KSI) przez pracowników Łódzkiego Urzędu Wojewódzkiego w Łodzi, a w szczególności spełnianie przez Wojewodę Łódzkiego warunków określonych w art. 453 ust. 1 i 2 ustawy oraz realizacja przez Wojewodę Łódzkiego przepisów rozporządzeń Ministra Spraw Wewnętrznych i Administracji w tym zakresie oraz Polityki Bezpieczeństwa Krajowego Systemu Informatycznego (KSI) Centralnego Organu Technicznego dla Organów i Służb poziom wysoki wersja 2.0. Kontrolowany okres to 01.01.2024 r. – 30.09.2024 r.

Podczas oceny spełniania przez kontrolowany podmiot warunków określonych w art. 453 ust. 1 i 2 ustawy o cudzoziemcach, zespół kontrolny wziął pod uwagę następujące kategorie:

[1] Z dniem 31.12.2024 r. za porozumieniem stron zmieniono formę zatrudnienia pana Piotra Piechowiaka z umowy o pracę na umowę zlecenie.

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

Pismem z dnia 02.05.2014 r. Wojewoda Łódzki wystąpił do Szefa Urzędu do Spraw Cudzoziemców (dalej: Szef Urzędu) z wnioskiem na podstawie art. 453 ustawy o cudzoziemcach o wyrażenie zgody na udostępnienie danych przetwarzanych w krajowym zbiorze rejestrów, ewidencji i wykazu w sprawach cudzoziemców za pomocą urządzeń telekomunikacyjnych. Organ wnioskujący oświadczył, że spełnia warunki wskazane w art. 453 ustawy o cudzoziemcach, tj.:

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

Decyzją z dnia 02.05.2014 r. nr 3/2014 Szef Urzędu na podstawie art. 454 ust. 1 ustawy o cudzoziemcach wyraził zgodę na udostępnienie Wojewodzie Łódzkiemu danych przetwarzanych w krajowym zbiorze rejestrów, ewidencji i wykazu w sprawach cudzoziemców za pomocą urządzeń telekomunikacyjnych.

Według stanu na dzień 12.11.2024 r. w podmiocie podlegającym kontroli aktywnych było 119 kont w systemie teleinformatycznym Pobyt v.3, za pośrednictwem którego użytkownicy indywidualni uzyskują dostęp do krajowego zbioru rejestrów, ewidencji i wykazu w sprawach cudzoziemców. Z informacji przekazanych przez Biuro Informatyki Urzędu do Spraw Cudzoziemców (dalej: Biuro Informatyki Urzędu) wynika również, że 3 użytkowników indywidualnych z Łódzkiego Urzędu Wojewódzkiego w Łodzi w okresie od 01.01.2024 r. do 30.09.2024 r. nie logowało się do systemu teleinformatycznego Pobyt.

Z wyjaśnień Pana Pawła Kowalczyka, Dyrektora Wydziału Spraw Cudzoziemców ŁUW, przedstawionych w piśmie z dnia 20.11.2024 r. nr: S.C.-II.6156.68.2024 r.[2], wynika, iż spośród trzech pracowników, którzy nie logowali się w systemie teleinformatycznym Pobyt, jeden pracownik, Pan Piotr Laskowski posiada uprawnienia do korzystania z systemu Pobyt dopiero od 07.10.2024 r. Pozostałe dwie osoby są pracownikami Wydziału Spraw Obywatelskich i realizują zadania w ramach postępowań o wydanie zezwolenia na pracę. Pani Martyna Strzelak przebywa na długotrwałym zwolnieniu lekarskim, a Pan Krzysztof Grausam podczas oddelegowania do innego Oddziału korzystał z systemu Pobyt, jednak jego obecny zakres obowiązków nie obejmuje przetwarzania danych w KZR; jego uprawnienia zostały cofnięte. Dyrektor Biura Informatyki Urzędu do Spraw Cudzoziemców potwierdził fakt cofnięcia w dniu 19.11.2024 r. uprawnień panu Krzysztofowi Grausam.

Odnosząc się do kwestii szkoleniowych oraz dostępu do przetwarzania danych osobowych, Dyrektor Wydziału Spraw Cudzoziemców ŁUW wyjaśnił, iż każdy nowo zatrudniony pracownik jest przeszkolony w zakresie przetwarzania danych osobowych oraz posiada upoważnienia do dostępu i przetwarzaniach danych osobowych w ramach Łódzkiego Urzędu Wojewódzkiego w Łodzi. Wszystkie osoby uzyskujące dostęp do systemu Pobyt mają obowiązek zapoznania się z treścią Instrukcji Zarządzania Systemem Teleinformatycznym Pobyt nr DKBM.WBOIN.2703.84.2022/WW, który to obowiązek realizują. W Wydziale Spraw Cudzoziemców nie jest prowadzony wykaz osób, które powinny zapoznać się z ww. polityką.

[2] Dalej: pismo nr: S.C.-II.6156.68.2024 r.

Brak wykazu osób, które zapoznały się z aktualną Instrukcją Zarządzania Systemem Teleinformatycznym Pobyt uznano za uchybienie.

Podmiot kontrolowany poinformował zespół kontrolny[3], iż jednym z elementów szkoleń pracowników w zakresie użytkowania SIS i VIS, bezpieczeństwa i jakości danych, praw podstawowych oraz procedur regulujących przetwarzanie danych, jest omówienie polityki ochrony danych osobowych, przetwarzanych poprzez KSI dla organów i służb, której treść jest udostępniona przez Komendanta Głównego Policji. Szkolenia prowadzone są przez wyznaczonych i wykwalifikowanych instruktorów w Łódzkim Urzędzie Wojewódzkim w Łodzi. Jednostka kontrolowana przekazała wykaz osób, które odbyły stosowne szkolenie oraz zaświadczenia potwierdzające ukończenie kursu[4]. Przy tym poinformowano zespół kontrolny, iż pracownicy Wydziału Spraw Cudzoziemców nie korzystają z SIS i VIS z poziomu systemu Pobyt, tylko wykorzystują karty mikroprocesorowe oraz działającą niezależnie od SI Pobyt aplikację siswww, której administratorem jest Komendant Główny Policji.

Z uwagi na fakt, że podmiot kontrolowany nie korzysta z dostępu do KSI za pośrednictwem systemu informatycznego Pobyt, lecz poprzez odrębną aplikację, która nie jest administrowana przez Szefa Urzędu do Spraw Cudzoziemców, odstąpiono od kontroli w zakresie dostępu do KSI.

Ponadto z wyjaśnień złożonych przez Dyrektora Wydziału Spraw Cudzoziemców[5] wynika, że podmiot kontrolowany wprowadził techniczne i organizacyjne zabezpieczenia stanowisk dostępowych do KZR i KSI, mające na celu uniemożliwienie dostępu osobom nieuprawnionym do przetwarzania danych osobowych oraz wykorzystywania ich niezgodnie z celem ich uzyskania. Ponadto prowadzi wykaz pomieszczeń, z których realizowany jest dostęp do KZR za pośrednictwem systemu teleinformatycznego POBYT. Zespołowi kontrolnemu przekazano kopię tego dokumentu[6].

Zabezpieczenia techniczne

Jednym z zastosowanych zabezpieczeń jest kontrola fizycznego dostępu do pomieszczeń, w których znajdują się stanowiska dostępowe do KZR i KSI. Kontrola ta realizowana jest przez pracowników ochrony, którzy wydają klucze do tych pomieszczeń wyłącznie uprawnionym pracownikom Wydziału.

Dostęp do systemu Pobyt jest zabezpieczony poprzez indywidualne uwierzytelnienie użytkownika za pomocą loginu i hasła. System wymusza cykliczną zmianę hasła w regularnych odstępach czasu. Ponadto komputery z dostępem do KZR i KSI są podłączone wyłącznie do wewnętrznej sieci Urzędu, która jest odseparowana od sieci publicznej. Każda stacja robocza z dostępem do KZR i KSI jest objęta ochroną za pomocą zapory Windows Defender. Nadzór nad siecią oraz zabezpieczenie systemów teleinformatycznych sprawuje Biuro Administracji i Logistyki Łódzkiego Urzędu Wojewódzkiego w Łodzi.

Zabezpieczenia organizacyjne

Dostęp do danych zgromadzonych w KZR i KSI jest przyznawany wyłącznie pracownikom, których zakres obowiązków wymaga przetwarzania tych danych. Przyznanie dostępu do systemu Pobyt następuje na podstawie pisemnego upoważnienia wydanego przez Dyrektora Wydziału, uprawniającego do dostępu do krajowego zbioru rejestrów, ewidencji i wykazu w sprawach cudzoziemców oraz wykorzystywania danych zawartych w tym rejestrze.

*

* *

[3] Pismo nr: S.C.-II.6156.68.2024 r.

[4] Załącznik do pisma nr: S.C.-II.6156.68.2024 r. – lista użytkowników systemów SIS i VIS w Oddziale Cudzoziemców do Spraw Legalizacji Pobytu i Pracy Wydziału Spraw Cudzoziemców; lista użytkowników systemów SIS i VIS Oddziale Cudzoziemców do Spraw Legalizacji Pobytu Wydziału Spraw Cudzoziemców; lista użytkowników systemów SIS i VIS w Oddziale Spraw Obywatelskich Wydziału Spraw Obywatelskich.

[5] Pismo nr: S.C.-II.6156.68.2024.

[6] Załącznik do pisma nr: S.C.-II.6156.68.2024 r.

W toku kontroli zespół kontrolny dokonał oględzin w siedzibie Wydziału Spraw Cudzoziemców Łódzkiego Urzędu Wojewódzkiego w Łodzi, w której zlokalizowane są stanowiska dostępowe do KZR[7]. Podczas oględzin zweryfikowano wszystkie pomieszczenia, w których znajdują się stanowiska dostępowe pod kątem zabezpieczeń uniemożliwiające dostęp osób nieuprawnionych do przetwarzania danych osobowych i wykorzystywania danych z KZR i KSI niezgodnie z celem ich uzyskania. Ponieważ skrzydło budynku, w którym znajduje się serwerownia jest w trakcie remontu, zespół kontrolny nie miał dostępu do budynku serwerowni i nie przeprowadził stosownych oględzin. Przyjęto informacje dotyczące zabezpieczeń, przekazane ustnie przez Pana Patryka Patucha z zespołu informatyków ŁUW.

Zabezpieczenia organizacyjne.

Zespół kontrolny nie miał zastrzeżeń co do zastosowanych zabezpieczeń organizacyjnych pomieszczeń ŁUW, w których zlokalizowane są stanowiska komputerowe, z których możliwy jest dostęp do KZR oraz KSI.

Zabezpieczenia techniczne.

W ramach sprawdzenia zabezpieczeń technicznych przeprowadzono oględziny sześciu stanowisk komputerowych użytkowników usytuowanych w różnych pomieszczeniach w siedzibie WSC ŁUW. Wyrywkową kontrolę uzasadniały ustne wyjaśnienia złożone przez Pana Przemysława Rusinkiewicza, informatyka WSC ŁUW, z których wynikało, że na każdym stanowisku zastosowane są takie same rozwiązania i zabezpieczenia, co potwierdziły oględziny.

W ramach oględzin 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. Przeprowadzono rozmowy z użytkownikami końcowymi KZR oraz z administratorem sieci.

Na podstawie oględzin wybranych stanowisk oraz wyjaśnień pana Przemysława Rusinkiewicza ustalono, iż:

- wszyscy użytkownicy korzystają z jednego, lokalnego konta Windows (zainstalowany system operacyjny to Windows 10 – licencja przypisana jest sprzętowo do płyty głównej każdego komputera), wspólnego dla wszystkich użytkowników, takiego samego na każdym stanowisku, z ustalonym na stałe hasłem, takim samym na każdym komputerze,
- logowanie do systemu teleinformatycznego Pobyt odbywa się w sposób zindywidualizowany, poprzez wpisanie przez każdego uprawnionego użytkownika loginu (nr PESEL) oraz hasła,
- na stacjach umożliwiających użytkownikom dostęp do systemu teleinformatycznego Pobyt brak jest aktualnych definicji programu antywirusowego, jak również aktualizacje Windows nie są systematycznie instalowane,
- ekrany monitorów użytkowników nie blokują się samoczynnie po bezczynności, natomiast po 30 minutach bezczynności włącza się wygaszacz ekranu,
- po 30 minutach bezczynności wygasa sesja w systemie teleinformatycznym Pobyt i wymagane jest ponowne zalogowanie się do systemu,
- na stanowiskach z dostępem do KZR nie ma możliwości korzystania z Internetu,
- na żadnym ze sprawdzonych stanowisk użytkownik nie posiada uprawnień administratora.

W wyniku przeprowadzonej kontroli stwierdzono następujące nieprawidłowości w zakresie zabezpieczeń systemu teleinformatycznego Pobyt:

- brak wykazu osób, które zapoznały się Zarządzania Systemem Teleinformatycznym POBYT nr DKBM.WBOIN.2703.84.2022/WW,

[7] Protokół z oględzin z dnia 29.11.2024 r.

- brak aktualnych definicji oprogramowania antywirusowego na stanowiskach dostępowych,
- brak systematycznej instalacji aktualizacji systemu operacyjnego Windows,
- brak automatycznej blokady ekranów monitorów użytkowników po okresie bezczynności,
- korzystanie z jednego, lokalnego konta użytkownika systemu operacyjnego wspólnego dla wszystkich użytkowników, identycznego na każdym stanowisku, z ustalonym na stałe hasłem, takim samym na wszystkich komputerach.

Powyższe należy potraktować jako uchybienie, za które odpowiedzialność ponosi administrator systemów informatycznych Łódzkiego Urzędu Wojewódzkiego w Łodzi.

Brak indywidualizacji dostępu do systemu, a także niestosowanie odpowiednich zabezpieczeń, takich jak aktualizacje oprogramowania czy oprogramowanie antywirusowe, naraża system na potencjalne ataki z sieci, wirusy czy inne formy cyberzagrożeń. Dodatkowo, brak blokady ekranów po okresie bezczynności i wspólne konto użytkowników utrudniają kontrolowanie dostępu do danych, co może prowadzić do nieautoryzowanego dostępu i utraty poufności informacji. Uznać należy, że stwierdzone uchybienia, choć nie miały charakteru jednostkowego, wpływały na kontrolowaną działalność w ograniczonym zakresie, stwarzając jednakowoż ryzyko naruszenia zasad bezpieczeństwa informatycznego, w tym ochrony danych osobowych.

W związku z powyższym, należy ocenić pozytywnie z uchybieniami realizację przez Wojewodę Łódzkiego 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. Uchybienia te powinny zostać niezwłocznie usunięte.

Zalecenia i wnioski pokontrolne.

W związku ze stwierdzonymi w toku kontroli uchybieniami w zakresie zabezpieczeń systemu teleinformatycznego Pobyt, zaleca się podjęcie niezwłocznych działań w celu ich usunięcia oraz zapewnienia właściwego poziomu bezpieczeństwa systemów informatycznych. W szczególności należy:

1. **Założyć i prowadzić wykaz osób**, które zapoznały się z aktualną Instrukcją Zarządzania Systemem Teleinformatycznym Pobyt.
2. **Zainstalować i aktualizować na bieżąco oprogramowanie antywirusowe** na wszystkich stanowiskach dostępowych do systemu teleinformatycznego Pobyt.
3. **Wprowadzić systematyczną instalację aktualizacji systemu operacyjnego Windows**, zapewniając jego bieżącą ochronę przed zagrożeniami.
4. **Skonfigurować automatyczną blokadę ekranów monitorów użytkowników** po określonym czasie bezczynności, aby zapobiec nieautoryzowanemu dostępowi.
5. **Zlikwidować praktykę korzystania z jednego, lokalnego konta Windows wspólnego dla wszystkich użytkowników** i wdrożyć indywidualne konta użytkowników z unikalnymi, okresowo zmienianymi silnymi hasłami.
6. **Zapewnić zgodność polityki bezpieczeństwa systemów informatycznych z obowiązującymi przepisami oraz dobrymi praktykami w zakresie ochrony danych i dostępu do systemów.**

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: biuroinformatyki@udsc.gov.pl.

Proszę o poinformowanie mnie o sposobie realizacji zaleceń pokontrolnych w terminie do dnia 25.04.2025 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 pisemnie 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.

.....
podpis kierownika zespołu kontrolnego

.....
pieczątka imienna i podpis kierownika podmiotu kontrolowanego

NACZELNIK WYDZIAŁU KONTROLI I NADZORU Biuro Szefa Urzędu Urząd do Spraw Cudzoziemców Krystyna KOMORNIAK

.....
podpis członka zespołu kontrolnego

M. Gosiak

.....
podpis członka zespołu kontrolnego

W przypadku odmowy podpisania protokołu – wzmianka o tym fakcie:

.....

.....

.....

.....

.....

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.