GENERALNY INSPEKTOR OCHRONY DANYCH OSOBOWYCH

Warszawa, dnia 12 września 2017 r.

DIS/DEC-1110/17/68986

dot. […]

D E C Y Z J A

Na podstawie art. 104 § 1 ustawy z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego (Dz. U. z 2017 r., poz. 1257), art. 12 pkt 2, art. 18 ust. 1 pkt 1 i art. 22 w związku z art. 36 ust. 1 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2016 r., poz. 922), po przeprowadzeniu postępowania administracyjnego w sprawie przetwarzania przez Ministra Cyfryzacji danych osobowych,

nakazuję Ministrowi Cyfryzacji usunięcie uchybień w procesie przetwarzania danych osobowych, poprzez:

1. **Opracowanie i wdrożenie procedur określających sposób postępowania po zgłoszeniu wystąpienia incydentu związanego z ochroną danych osobowych przetwarzanych w ramach rejestru PESEL, w terminie do 31 grudnia 2017 r.**
2. **Zapewnienie, aby jednemu użytkownikowi nie mogła zostać wydana więcej niż jedna karta z certyfikatem umożliwiającym dostęp do rejestru PESEL za pomocą urządzeń teletransmisji danych, w terminie do 30 września 2017 r.**
3. **Modyfikację aplikacji „A.", za pośrednictwem której realizowany jest dostęp do rejestru PESEL, w taki sposób, aby umożliwiała ona podanie uzasadnienia dla dokonywanego sprawdzenia danych w rejestrze PESEL, w terminie do 31 marca 2018 r.**
4. **Wdrożenie oprogramowania służącego do analizy logów systemowych, w tym operacji dokonywanych przez użytkowników, którym przyznany został dostęp do rejestru PESEL, w terminie do 31 grudnia 2017 r.**

ul. Stawki 2
00-193 Warszawa

tel. 22 531-03-08
22 531-03-13
fax 22 531-03-01
www.giodo.gov.pl

U z a s a d n i e n i e

Inspektorzy upoważnieni przez Generalnego Inspektora Ochrony Danych Osobowych, przeprowadzili w Ministerstwie Cyfryzacji z siedzibą w Warszawie przy ul. Królewskiej 27 kontrolę zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych sygn. […], tj. ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2016 r., poz. 922), zwaną dalej ustawą, i rozporządzeniem 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), zwanym dalej rozporządzeniem. Zakresem kontroli objęto przetwarzanie danych osobowych przez Ministra Cyfryzacji w zbiorze danych osobowych o nazwie „R.”, w tym udostępnianie danych z rejestru PESEL komornikom sądowym. W toku kontroli odebrano od pracowników Ministerstwa Cyfryzacji ustne wyjaśnienia, skontrolowano systemy informatyczne oraz dokonano oględzin pomieszczeń, w których odbywa się przetwarzanie danych osobowych. Stan faktyczny został szczegółowo opisany w protokole kontroli, który został podpisany przez Ministra Cyfryzacji.

Na podstawie tak zgromadzonego materiału dowodowego ustalono, że w procesie przetwarzania danych osobowych Minister Cyfryzacji, jako administrator danych, naruszył przepisy o ochronie danych osobowych. Uchybienia te polegały na:

1. Braku procedur określających sposób postępowania po zgłoszeniu wystąpienia incydentu związanego z ochroną danych osobowych przetwarzanych w ramach rejestru PESEL.
2. Istnieniu możliwości przyznania jednemu użytkownikowi więcej niż jednej karty z certyfikatem umożliwiającym dostęp do rejestru PESEL za pomocą urządzeń teletransmisji danych.
3. Niezapewnianiu przez aplikację „A.”, za pośrednictwem której realizowany jest dostęp do rejestru PESEL, możliwości podania uzasadnienia dla dokonywanego sprawdzenia danych w rejestrze PESEL.
4. Niewdrożeniu oprogramowania służącego do analizy logów systemowych, w tym operacji dokonywanych przez użytkowników, którym przyznany został dostęp do rejestru PESEL.

W związku z powyższym, w dniu 17 sierpnia 2017 r. Generalny Inspektor Ochrony Danych Osobowych wszczął z urzędu postępowanie administracyjne w niniejszej sprawie w celu wyjaśnienia okoliczności sprawy sygn. […].

W odpowiedzi na zawiadomienie o wszczęciu postępowania administracyjnego Minister Cyfryzacji pismem z dnia 28 sierpnia 2017 r., sygn. […] złożył wyjaśnienia, w których poinformowano, że:

1. Z uwagi na identyfikację konieczności realizacji zadań niezbędnych do zapewnienia odpowiedniego poziomu bezpieczeństwa systemu i danych gromadzonych w poszczególnych rejestrach, w ramach Systemu „X.”, po przeprowadzeniu analiz, Ministerstwo Cyfryzacji zwróciło się do Ministra Rozwoju i Finansów o uruchomienie rezerwy celowej pn. […] i zwiększenie planu wydatków na rok 2017. Powyższe środki zostaną przeznaczone na sfinansowanie m.in. tych zadań, których niezbędność realizacji wskazał Generalny Inspektor.
2. Część środków z rezerwy celowej zostanie przeznaczona m.in. na opracowanie polityki bezpieczeństwa „X.”. Wdrożenie opracowanej w tym roku polityki bezpieczeństwa planowane jest w 2018 r. Przekazany przez C. wstępny harmonogram przygotowania polityki bezpieczeństwa „X.” określa, że jeszcze we wrześniu br. zostanie zakończona analiza stanu obecnego, zdiagnozowane zostaną potencjalne zagrożenia i ryzyka, przeprowadzone zostaną warsztaty ze specjalistami w poszczególnych obszarach technicznych. W październiku 2017 r. opracowane zostaną główne zasady polityki bezpieczeństwa dla wszystkich systemów w ramach „X.”, natomiast do grudnia br. nastąpi opracowanie polityk dziedzinowych, wyspecyfikowanych dla poszczególnych rejestrów.
3. Podjęto działania mające na celu niezwłoczną zmianę zapisów polityk certyfikacji dla operatorów oraz infrastruktury „X.”. Nowe wersje polityk nie będą dopuszczały możliwości wydania przez operatorów Centrum C. więcej niż jednego ważnego certyfikatu. W konsekwencji, w przypadku wystąpienia z wnioskiem o dostęp użytkownika zostanie uruchomiona procedura weryfikacji, czy użytkownik nie posiada ważnego certyfikatu na te same dane. W sytuacji gdy okaże się, że użytkownik posiada już przynajmniej jeden ważny certyfikat, dotychczasowe certyfikaty zostaną unieważnione. Zakończenie aktualizacji polityk certyfikacji dla operatorów oraz infrastruktury „X.” nastąpi w terminie do 31 sierpnia 2017 r. Następnie dokumenty zostaną opublikowane na stronie Ministerstwa Cyfryzacji oraz rozesłane na aktualne adresy e-mail lokalnych administratorów systemu celem stosowania przez użytkowników „X.”.
4. Odnosząc się do kwestii obowiązku podawania przez podmioty posiadające dostęp do rejestru PESEL w trybie teletransmisji danych uzasadnienia dla ich pozyskania nie można nie zauważyć, że przedmiotowe wymaganie nie wynika z przepisów prawa. Wydając decyzję administracyjną przyznającą uprawnionemu podmiotowi dostęp do rejestru PESEL zastrzega się, stosownie do treści art. 46 ust. 1 ustawy z dnia 24 września 2010 r. o ewidencji ludności (Dz. U. z 2017 r., poz. 657), że dane mogą być wykorzystane wyłącznie do realizacji zadań ustawowych tego

podmiotu. Należy przy tym zwrócić uwagę, że obecne przepisy ustawy o ewidencji ludności nie przewidują, w przeciwieństwie do uchylonych przepisów ustawy o ewidencji ludności i dowodach osobistych, ażeby stosowane urządzenia lub systemy umożliwiały identyfikację celu uzyskania danych. Również z przepisów rozporządzenia Ministra Spraw Wewnętrznych i Administracji w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych nie wynika konieczność odnotowywania przez system teleinformatyczny parametrów innych niż w nim wskazane. Warto również wskazać, że w przypadku realizowania przez służby pewnych czynności operacyjnych nie zawsze będzie możliwe wpisanie w aplikacji dostępowej do rejestru PESEL sygnatury akt sprawy, a tym bardziej uzasadnienia. Należy także zwrócić uwagę na fakt, że takie rozwiązanie będzie możliwe do zastosowania wyłącznie wobec podmiotów, które dostęp do danych zgromadzonych w rejestrze PESEL mają za pośrednictwem aplikacji „A.”. Spowoduje to zróżnicowanie podmiotów w zakresie zasad dostępu do prowadzonych rejestrów, co nie znajduje odzwierciedlenia w przepisach prawa.

5. Mając jednak na względzie rekomendację Generalnego Inspektora, C. zlecono analizę możliwości technicznych wdrożenia zmiany w aplikacji „A.” polegającej na odnotowaniu uzasadnienia dostępu do danych lub sygnatury sprawy. Z uwagi na fakt, że zaplanowany na 2017 r. budżet dla „X.”, jak i wniosek o uruchomienie rezerwy celowej nie przewidywał finansowania tej modyfikacji, jej realizacja będzie możliwa z rezerwy celowej zabezpieczonej na 2018 r. Dlatego planowany, realny termin wdrożenia zmiany to III kwartał 2018 r.
6. Wdrożenie systemów informatycznych do analizy logów systemowych ujęto we wniosku o uruchomienie rezerwy celowej na 2017 r., a samo oprogramowanie zostało już przez Ministerstwo Cyfryzacji zakupione. Ponadto, w związku z koniecznością zwiększenia zdolności monitorowania i zarządzania bezpieczeństwem systemów planowany jest zakup komponentów, które pozwolą ten cel zrealizować. Niezależnie od powyższego należy wskazać, że „X.” jest monitorowany w trybie ciągłym i zapewnia bezpieczeństwo w procesach udostępniania danych z rejestru PESEL.

Po zapoznaniu się z całością materiału dowodowego zebranego w sprawie Generalny Inspektor Ochrony Danych Osobowych zważył co następuje:

Zgodnie z art. 36 ust. 1 ustawy o ochronie danych osobowych, administrator danych jest obowiązany zastosować środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności powinien zabezpieczyć dane przed ich udostępnieniem osobom

nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem.

W odpowiedzi na zawiadomienie o wszczęciu postępowania administracyjnego Minister Cyfryzacji szeroko przedstawił podjęte działania o charakterze organizacyjnym i technicznym (i źródła ich finansowania) mające zapewnić ochronę danych osobowych przetwarzanych w ramach rejestru PESEL i doprowadzić do usunięcia stwierdzonych w toku kontroli nieprawidłowości w procesie przetwarzania danych osobowych, tj. działania zmierzające do:

- wdrożenia procedur określających sposób postępowania po zgłoszeniu wystąpienia incydentu związanego z ochroną danych osobowych przetwarzanych w ramach rejestru PESEL, w ramach polityki bezpieczeństwa dla „X.”,
- wyeliminowania możliwości przyznania jednemu użytkownikowi więcej niż jednej karty z certyfikatem umożliwiającym dostęp do rejestru PESEL za pomocą urządzeń teletransmisji danych,
- modyfikacji aplikacji „A.”, za pośrednictwem której realizowany jest dostęp do rejestru PESEL, tak aby zapewniała możliwość podania uzasadnienia dla dokonywanego sprawdzenia danych w rejestrze PESEL,
- wdrożenia oprogramowania służącego do analizy logów systemowych, w tym operacji dokonywanych przez użytkowników, którym przyznany został dostęp do rejestru PESEL.

Podjęcie tych działań nie może zostać jednak uznane za przywrócenie stanu zgodnego z prawem. Nadal bowiem uchybienia stwierdzone w toku kontroli przeprowadzonej w Ministerstwie Cyfryzacji nie zostały usunięte. Tym niemniej, przy zakreślaniu terminów na usunięcie uchybień należało wziąć pod uwagę uwarunkowania organizacyjne i finansowe, w których funkcjonuje Minister Cyfryzacji, i uwzględnić zadeklarowane w odpowiedzi na zawiadomienie o wszczęciu postępowania administracyjnego terminy na przywrócenie stanu zgodnego z prawem, za wyjątkiem terminu zaproponowanego do usunięcia nieprawidłowości polegającej na braku zapewnienia przez aplikację „A.” możliwości podania uzasadnienia dla dokonywanego sprawdzenia danych w rejestrze PESEL. W tym bowiem przypadku, termin podany przez Ministra Cyfryzacji w piśmie stanowiącym odpowiedź na zawiadomienie o wszczęciu postępowania administracyjnego (III kwartał 2018 r.) jest terminem zbyt odległym biorąc pod uwagę istniejące zagrożenia związane z brakiem wskazanej funkcjonalności w aplikacji „A.”, tj. przede wszystkim możliwością dokonywana sprawdzeń danych w rejestrze PESEL bez związku z prowadzoną sprawą i wykorzystania ich w sposób niezgodny z obowiązującym prawem. Z tego względu istotne jest jak najszybsze zakończenie działań skutkujących wyposażeniem ww. aplikacji w przedmiotową funkcjonalność, tak aby to zagrożenie zostało wyeliminowane (lub znacznie

ograniczone) w możliwie najkrótszym czasie. W ocenie Generalnego Inspektora, powinno to nastąpić najpóźniej do 31 marca 2018 r. Przeciw uwzględnieniu zaproponowanego terminu przemawia także fakt, iż Minister Cyfryzacji o istnieniu omawianego uchybienia został poinformowany w piśmie z dnia 30 marca 2017 r., sygn. […]. Było zatem wystarczająco dużo czasu, aby zabezpieczyć na 2017 r. niezbędne środki finansowe do przeprowadzenia modyfikacji aplikacji „A.” w tym zakresie.

W piśmie stanowiącym odpowiedź na zawiadomienie o wszczęciu postępowania administracyjnego Minister Cyfryzacji podniósł, że obowiązek podawania przez podmioty uprawnione do dostępu do rejestru PESEL uzasadnienia dla dokonywanego w tym rejestrze sprawdzenia danych nie wynika z przepisów prawa. Ustosunkowując się do tego stwierdzenia wskazać należy, że rzeczywiście takiego obowiązku nie zawierają przepisy ustawy o ewidencji ludności. Można go natomiast wywieść z treści art. 36 ust. 1 ustawy o ochronie danych osobowych, który zobowiązuje administratora danych do zastosowania takich środków technicznych i organizacyjnych, które zapewnią ochronę przetwarzanym danym osobowym odpowiednią do zagrożeń. Skoro jednym z już zidentyfikowanych zagrożeń dla danych przetwarzanych w ramach rejestru PESEL jest możliwość dokonywania sprawdzeń w tym rejestrze przez podmioty uprawnione bez związku z prowadzoną sprawą, to oczywistym jest, że konieczne jest podjęcie przez administratora danych działań niezbędnych do wyeliminowania (lub co najmniej ograniczenia) takiej praktyki.

Wdrożenie w aplikacji „A.”, za pośrednictwem której jest realizowany dostęp do rejestru PESEL, funkcjonalności wymuszającej podawania uzasadnienia dla dokonywanego sprawdzenia, np. w postaci sygnatury sprawy, jest najbardziej odpowiednim sposobem przeciwdziałania ww. praktykom. Efektem wdrożenia tej funkcjonalności będzie bowiem możliwość stwierdzenia, czy osoba dokonująca sprawdzenia danych w rejestrze PESEL uczyniła to na potrzeby prowadzonej sprawy, czy też bez związku z nią. Zatem, wyposażenie aplikacji „A.” w omawianą funkcjonalność będzie skutkowało eliminacją (lub ograniczeniem) jednego z zagrożeń dla danych przetwarzanych w rejestrze PESEL, a tym samym będzie stanowiło realizację obowiązku wynikającego z art. 36 ust. 1 ustawy o ochronie danych osobowych.

Należy się zgodzić z Ministrem Cyfryzacji, że nie zawsze przy dokonywaniu sprawdzenia danych w rejestrze PESEL będzie możliwe podanie pełnego uzasadnienia dla takiego sprawdzenia. Tak może być np. w przypadku służb prowadzących czynności operacyjne. Wskazać jednak należy, że wpisanie przez taką służbę „czynności operacyjne” lub „rozpoznanie” jako uzasadnienie dla dokonywanego sprawdzenia też stanowi uzasadnienie i jako takie może pozwolić na przeprowadzenie weryfikacji, czy sprawdzenie rzeczywiście miało miejsce w związku z prowadzonymi czynnościami operacyjnymi.

Kontrola przeprowadzona w Ministerstwie Cyfryzacji była następstwem kontroli przeprowadzonych u komorników sądowych, u których stwierdzono pobieranie znacznych ilości danych z rejestru PESEL. Każdy z poddanych kontroli komorników do sprawdzania danych w rejestrze PESEL wykorzystywał aplikację „A.”. Nie dysponując zatem ustaleniami dotyczącymi realizowania przez podmioty uprawnione dostępu do rejestru PESEL za pośrednictwem własnych systemów informatycznych, a w szczególności ustaleniami odnośnie funkcjonalności tych systemów, trudno jest ustosunkować się do stwierdzenia Ministra Cyfryzacji zawartego w piśmie stanowiącym odpowiedź na zawiadomienie o wszczęciu postepowania administracyjnego, że wdrożenie w aplikacji „A.” funkcjonalności pozwalającej na podawanie uzasadnienia dla dokonywanego sprawdzenia danych w rejestrze PESEL spowoduje zróżnicowanie podmiotów korzystających z tej aplikacji w stosunku do podmiotów korzystających z własnych systemów informatycznych w zakresie zasad dostępu do rejestru PESEL.

Wobec powyższego, Generalny Inspektor Ochrony Danych Osobowych rozstrzygnął jak w sentencji.

Na podstawie art. 127 § 3 Kodeksu postępowania administracyjnego w zw. z art. 21 ust. 1 ustawy o ochronie danych osobowych strona niezadowolona z niniejszej decyzji może, w terminie 14 dni od dnia jej doręczenia, złożyć do Generalnego Inspektora Ochrony Danych Osobowych wniosek o ponowne rozpatrzenie sprawy (adres: Biuro Generalnego Inspektora Ochrony Danych Osobowych, ul. Stawki 2, 00 – 193 Warszawa). W trakcie biegu terminu do wniesienia wniosku o ponowne rozpatrzenie sprawy strona może zrzec się prawa do jego wniesienia wobec organu administracji publicznej, który wydał decyzję. Z dniem doręczenia organowi administracji publicznej oświadczenia o zrzeczeniu się prawa do wniesienia wniosku o ponowne rozpatrzenie sprawy przez ostatnią ze stron postępowania, decyzja staje się ostateczna i prawomocna, co oznacza, iż decyzja podlega natychmiastowemu wykonaniu i brak jest możliwości zaskarżenia decyzji do Wojewódzkiego Sądu Administracyjnego. Nie jest możliwe skuteczne cofnięcie oświadczenia o zrzeczeniu się prawa do wniesienia odwołania.

Jeżeli strona nie zamierza korzystać z prawa do zwrócenia się z wnioskiem o ponowne rozpatrzenie sprawy, może wnieść do Wojewódzkiego Sądu Administracyjnego w Warszawie skargę na decyzję w terminie 30 dni od dnia doręczenia decyzji stronie. Skargę wnosi się za

pośrednictwem Generalnego Inspektora Ochrony Danych Osobowych. Wpis od skargi wynosi 200 złotych. Strona składająca skargę może ubiegać się o przyznanie prawa pomocy, które obejmuje zwolnienie od kosztów sądowych oraz ustanowienie adwokata, radcy prawnego, doradcy podatkowego lub rzecznika patentowego. Prawo pomocy może być przyznane na wniosek strony złożony przed wszczęciem postępowania lub w toku postępowania. Wniosek ten wolny jest od opłat sądowych.

W razie niewykonania decyzji w terminie zostanie wobec podmiotu zobowiązanego do jej wykonania wszczęte postępowanie egzekucyjne na podstawie przepisów ustawy z dnia 17 czerwca 1966 r. o postępowaniu egzekucyjnym w administracji (Dz. U. z 2016 r., poz. 599 z późn. zm.).