GENERALNY INSPEKTOR OCHRONY DANYCH OSOBOWYCH

Warszawa, 9 listopada 2017 *r.*

DIS/DEC- 1352/17/82128
dot. […]

D E C Y Z J A

Na podstawie art. 138 § 1 pkt 1 i 2 ustawy z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego (Dz. U. z 2017 r., poz. 1257) oraz 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 wniosku pełnomocnika Ministra Cyfryzacji o ponowne rozpatrzenie sprawy zakończonej decyzją Generalnego Inspektora Ochrony Danych Osobowych z 12 września 2017 r., nr DIS/DEC-1110/17/68986, nakazującą Ministrowi Cyfryzacji usunięcie uchybień w procesie przetwarzania danych osobowych,

1. **Uchylam pkt 2 decyzji z 12 września 2017 r., nr DIS/DEC-1110/17/68986, i umarzam postępowanie w tym zakresie.**
2. **Utrzymuję w mocy pkt 3 decyzji z 12 września 2017 r., nr DIS/DEC-1110/17/68986.**

Uzasadnienie

W dniu 12 września 2017 r. Generalny Inspektor Ochrony Danych Osobowych wydał decyzję nr DIS/DEC-1110/17/68986, nakazującą 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.

ul. Stawki 2
00-193 Warszawa

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

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.

W dniu 26 września 2017 r. do Biura Generalnego Inspektora Ochrony Danych Osobowych wpłynął, złożony w terminie, wniosek pełnomocnika Ministra Cyfryzacji o ponowne rozpatrzenie sprawy zakończonej decyzją Generalnego Inspektora nr DIS/DEC-1110/17/68986 w zakresie rozstrzygnięć ujętych w pkt 2 i 3 ww. decyzji i uchylenie jej w zaskarżonej części.

We wniosku o ponowne rozpatrzenie sprawy pełnomocnik Ministra Cyfryzacji podniósł, że:

1. Polityka certyfikacji dla operatorów oraz infrastruktury SRP w zakresie wydawania zduplikowanych certyfikatów dostępowych do rejestru PESEL została zmieniona z dniem 31 sierpnia 2017 r., a zatem orzekanie przez Generalnego Inspektora Ochrony Danych Osobowych w tym zakresie 12 września 2017 r. winno zakończyć się umorzeniem postępowania z uwagi na jego bezprzedmiotowość. Przedmiot postępowania administracyjnego musi istnieć przez cały czas trwania postępowania, od jego wszczęcia aż do jego zakończenia. Zatem, w sytuacji gdy Polityka certyfikacji dla operatorów oraz infrastruktury SRP została zmodyfikowana w sposób, który uniemożliwi wydanie jednemu użytkownikowi więcej niż jednego certyfikatu dostępowego do rejestru PESEL, Generalny Inspektor nie mógł orzekać w przedmiocie zapewnienia powyższego, poprzez nałożenie na Ministra Cyfryzacji nakazu uprzednio już zrealizowanego.
2. Udostępnienie danych osobowych z rejestrów publicznych następuje na podstawie przepisów regulujących funkcjonowanie tychże rejestrów. Z tego względu podawanie przez podmioty uprawnione i realizujące dostęp do rejestru PESEL w drodze teletransmisji danych uzasadnienia dla ich każdorazowego pozyskania jest niezgodne z obowiązującymi przepisami prawa. W wydanej decyzji organ nie polemizuje z powyższym stwierdzeniem, wskazując jednocześnie, że obowiązek powyższy można wywieść z treści art. 36 ust. 1 ustawy o ochronie danych osobowych.

3. Przypomnienia wymaga, że stosownie do treści art. 46 ust. 1 ustawy z dnia 24 września 2010 r. o ewidencji ludności (Dz. U. z 2017 r., poz. 657), dane mogą być wykorzystane wyłącznie do realizacji zadań ustawowych podmiotów wymienionych w tym przepisie. Zatem obowiązkiem Ministra Cyfryzacji jest udostępnienie danych, jeżeli są one niezbędne do osiągnięcia prawnie usprawiedliwionych celów.
4. Organ ochrony danych osobowych nie wskazał, w jaki sposób modyfikacja aplikacji „A.", która będzie wymagała podania uzasadnienia lub sygnatury akt sprawy, przełoży się na zwiększenie bezpieczeństwa przetwarzania danych przez podmioty uprawnione. Tymczasem obowiązek taki istnieje po stronie organu administracji publicznej na gruncie art. 8 i 11, a w szczególności art. 107 § 1 pkt 6 Kpa.
5. Wydając rozstrzygnięcie zawarte w pkt 3 decyzji organ ochrony danych osobowych nie wziął pod uwagę, że przedmiotowe rozwiązanie byłoby możliwe do zastosowania wyłącznie wobec podmiotów, które dostęp do danych zgromadzonych w rejestrze PESEL mają za pośrednictwem aplikacji „A.". Rekomendowane przez Generalnego Inspektora rozwiązanie nie znajdzie zastosowania w przypadku, w którym podmiot uzyskuje dostęp do danych za pomocą swojego systemu teleinformatycznego, na budowę którego resort cyfryzacji nie ma żadnego wpływu. Należy podkreślić, że doprowadziłoby to do zróżnicowania podmiotów wobec prawa.
6. Brak ustaleń w zakresie realizacji dostępu do rejestru PESEL przez podmioty uprawnione za pośrednictwem własnych systemów informatycznych narusza art. 7 Kpa. Nakaz sformułowany w pkt 3 decyzji dotyczy nie tylko kilku skontrolowanych kancelarii komorniczych, ale wszystkich podmiotów mających dostęp do rejestru PESEL. Dostęp ten, co nie stoi w sprzeczności z przepisami prawa, jest zróżnicowany i nie zawsze odbywa się za pośrednictwem aplikacji „A.", czego orzekając nie wziął pod uwagę organ ochrony danych osobowych.
7. Nie należy również zapominać o adekwatności przyjmowanych w dziedzinie ochrony danych osobowych rozwiązań do spodziewanych rezultatów. Rozwiązania te powinny być realizowane poprzez zastosowanie skutecznych środków technicznych i organizacyjnych. Skuteczność zastosowanych środków powinna natomiast podlegać badaniom, a w tym konkretnym przypadku badanie takie nie jest możliwe do zrealizowania.

Generalny Inspektor Ochrony Danych Osobowych zważył co następuje:

Z zarzutami zawartymi we wniosku o ponowne rozpatrzenie sprawy nie można się zgodzić. Przede wszystkim wskazać należy, że w piśmie stanowiącym odpowiedź na zawiadomienie o wszczęciu postępowania administracyjnego (pismo z 28 sierpnia 2017 r., nr […]) zawarta została

informacja o podjęciu działań mających na celu zmianę zapisów w Polityce certyfikacji dla operatorów oraz infrastruktury SRP tak, aby nie było możliwe wydanie więcej niż jednego certyfikatu temu samemu użytkownikowi. Samo podjęcie działań w celu usunięcia stwierdzonego w toku kontroli uchybienia nie mogło zostać uznane za przywrócenie stanu zgodnego z prawem. Działania te mogły bowiem nie zakończyć się aktualizacją ww. dokumentu w omawianym zakresie oraz wdrożeniem tej aktualizacji. Należy także wskazać, że kserokopia zaktualizowanej Polityki certyfikacji dla operatorów oraz infrastruktury SRP i wydruki potwierdzające jej wdrożenie wpłynęły do Biura Generalnego Inspektora Ochrony Danych Osobowych 18 października 2017 r. Dopiero wówczas można było dokonać oceny, czy wskazany dokument został zaktualizowany w zakresie zapewniającym przywrócenie stanu zgodnego z prawem, a przede wszystkim, czy został wdrożony.

Należy także wskazać, ze we wniosku o ponowne rozpatrzenie sprawy pełnomocnik Ministra Cyfryzacji akcentuje wyłącznie fakt dokonania aktualizacji Polityki certyfikacji dla operatorów oraz infrastruktury SRP przed dniem wydania zaskarżonej decyzji. Tymczasem dla stwierdzenia, czy został przywrócony stan zgodny z prawem w tym zakresie istotny jest również moment wdrożenia zaktualizowanego dokumentu. Z wydruku załączonego do pisma pełnomocnika Ministra Cyfryzacji z 16 października 2017 r., nr […], wynika, że informacja o zatwierdzeniu zaktualizowanej Polityki certyfikacji dla operatorów oraz infrastruktury SRP została przekazana lokalnym administratorom aplikacji „A.” 14 września 2017 r., tj. już po wydaniu decyzji przez Generalnego Inspektora Ochrony Danych Osobowych. Oznacza to, że w momencie wydawania zaskarżonej decyzji istniał przedmiot postępowania administracyjnego. Nie było zatem podstaw do umorzenia postępowania w tym zakresie.

Biorąc jednak pod uwagę, że z przedstawionej przez pełnomocnika Ministra Cyfryzacji zaktualizowanej Polityki certyfikacji dla operatorów oraz infrastruktury SRP wynika, że obecnie nie jest już możliwe wydanie więcej niż jednego certyfikatu temu samemu użytkownikowi, jak również, iż wskazany dokument został wdrożony, to uznać należy, że w tym zakresie przywrócony został stan zgodny z prawem. Należało zatem uchylić pkt 2 decyzji Generalnego Inspektora z 12 września 2017 r., nr DIS/DEC-1110/17/68986, i umorzyć postępowanie w tym zakresie.

Ustosunkowując się do kolejnych zarzutów pełnomocnika Ministra Cyfryzacji wskazać należy, że przepisy ustawy o ewidencji ludności rzeczywiście nie formułują wprost obowiązku podawania przez podmioty uprawnione do dostępu do rejestru PESEL uzasadnienia dla dokonywanego sprawdzenia danych w tym rejestrze, choć można próbować go wywieść z treści art. 48 pkt 2 powołanej ustawy, który nakłada na podmioty realizujące dostęp do rejestru PESEL za pomocą urządzeń teletransmisji danych obowiązek posiadania zabezpieczeń technicznych

i organizacyjnych właściwych dla przetwarzania danych osobowych, uniemożliwiających w szczególności wykorzystanie danych niezgodnie z celem ich uzyskania. Niewątpliwie środkiem, który uniemożliwi (lub co najmniej utrudni) wykorzystanie danych niezgodnie z celem ich uzyskania, jest wyposażenie aplikacji „A.” w funkcjonalność pozwalającą na odnotowanie uzasadnienia dla dokonywanego sprawdzenia danych w rejestrze PESEL. Z uwagi na to, że to Minister Cyfryzacji udostępnia aplikację „A.” podmiotom uprawnionym do dostępu do rejestru PESEL, to obowiązek zapewnienia, że aplikacja ta będzie spełniała wszystkie wymogi wynikające z przepisów prawa, w tym wymogi odnoszące się do przetwarzania danych osobowych pobieranych z rejestru PESEL, spoczywa właśnie na nim.

Kwestie odpowiedniego zabezpieczenia danych osobowych i obowiązków administratora danych w tym zakresie regulują jednak przede wszystkim przepisy ustawy o ochronie danych osobowych, a w szczególności art. 36 ust. 1 tej ustawy. Nakładają one na Ministra Cyfryzacji, jako administratora danych przetwarzanych w ramach rejestru PESEL, obowiązek zastosowania takich środków technicznych i organizacyjnych, które zapewnią ochronę danych osobowych 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. Nie ulega wątpliwości, że najbardziej odpowiednim sposobem przeciwdziałania ww. praktykom będzie wdrożenie w aplikacji „A.”, za pośrednictwem której jest realizowany dostęp do rejestru PESEL, funkcjonalności wymuszającej podawanie uzasadnienia dla dokonywanego sprawdzenia, np. w postaci sygnatury sprawy.

Z uwagi na to, że konieczność zaimplementowania w aplikacji „A.” omawianej funkcjonalności, jako środka służącego do wyeliminowania (lub ograniczenia) zagrożenia dla danych przetwarzanych w tym rejestrze, można wywieść zarówno z przepisów ustawy o ewidencji ludności, jak i z przepisów ustawy o ochronie danych osobowych, a więc z przepisów powszechnie obowiązujących, to nie można twierdzić, że takie rozwiązanie jest niezgodne z tymi przepisami.

We wniosku o ponowne rozpatrzenie sprawy pełnomocnik Ministra Cyfryzacji podniósł, że wyposażenie aplikacji „A.” w funkcjonalność pozwalającą na odnotowywanie uzasadnienia dla dokonywanego sprawdzenia danych w rejestrze PESEL spowoduje zróżnicowanie wobec prawa podmiotów realizujących ten dostęp przy użyciu ww. aplikacji w stosunku do tych podmiotów, które taki dostęp realizują przy wykorzystaniu własnych systemów informatycznych, w związku z powyższym zanegował konieczność jej wprowadzenia. Potencjalne zróżnicowanie podmiotów uprawnionych do dostępu do rejestru PESEL nie może jednak powodować zaniechania przez

administratora danych podejmowania działań zmierzających do zlikwidowania (lub co najmniej ograniczenia) zidentyfikowanego ryzyka dla danych przetwarzanych w ramach rejestru PESEL. Tymczasem, jak wynika z wniosku o ponowne rozpatrzenie sprawy, Minister Cyfryzacji wobec możliwości powstania takiego zróżnicowania postanowił zignorować zidentyfikowane już zagrożenie dla danych przetwarzanych w rejestrze PESEL i nie podejmować żadnych działań w celu jego eliminacji lub ograniczenia. Taka praktyka w świetle art. 36 ust. 1 ustawy o ochronie danych osobowych jest jednak niedopuszczalna. Odpowiedzialny administrator danych w takiej sytuacji nie powinien rezygnować z działań zapewniających prawidłową realizację obowiązków wynikających z ww. przepisu ustawy o ochronie danych osobowych. W przypadku gdy w jego opinii może to spowodować powstanie zróżnicowania podmiotów w sposobie realizacji dostępu do rejestru PESEL, to zamiast zignorować istniejące zagrożenie powinien podjąć działania w celu przeciwdziałania takiemu zróżnicowaniu. Przykładem takiego działania może być opracowanie wytycznych dla podmiotów korzystających przy dostępie do rejestru PESEL z własnych systemów informatycznych, w tym wskazówek, jak interpretować wynikający z art. 48 pkt 2 ustawy o ewidencji ludności wymóg posiadania zabezpieczeń technicznych i organizacyjnych uniemożliwiających wykorzystanie danych niezgodnie z celem ich uzyskania. Należy bowiem w tym miejscu zauważyć, że obowiązek określony w ww. przepisie ustawy o ewidencji ludności odnosi się nie tylko do podmiotów, które przy dostępie do rejestru PESEL korzystają z udostępnionej przez Ministra Cyfryzacji aplikacji „A.”, ale także tych podmiotów, które dostęp ten realizują za pomocą własnego systemu informatycznego (a jak już wyżej wskazano, można z niego wywieść konieczność posiadania przez podmiot uprawniony do dostępu do rejestru PESEL systemu informatycznego wyposażonego w funkcjonalność pozwalającą na odnotowanie uzasadnienia dla dokonywanego sprawdzenia danych w tym rejestrze jako środka uniemożliwiającego lub utrudniającego wykorzystanie danych pobranych z tego rejestru niezgodnie z celem ich pobrania). Wreszcie, Minister Cyfryzacji może skorzystać z inicjatywy ustawodawczej w celu zmiany obowiązujących przepisów dotyczących rejestru PESEL.

Nie można się zgodzić z pełnomocnikiem Ministra Cyfryzacji, że w zaskarżonej decyzji nie wskazano, w jaki sposób wyposażenie aplikacji „A.” w funkcjonalność pozwalającą na podawanie uzasadnienia dla dokonywanego sprawdzenia danych w rejestrze PESEL przyczyni się do zwiększenia bezpieczeństwa danych. W uzasadnieniu decyzji wyraźnie przecież wskazano, że wprowadzenie tej funkcjonalności spowoduje wyeliminowanie lub co najmniej ograniczenie zagrożenia dla danych osobowych przetwarzanych w ramach rejestru PESEL, polegającego na dokonywaniu sprawdzeń danych w tym rejestrze bez związku z prowadzoną sprawą. W konsekwencji nie można mówić o naruszeniu art. 8, 11 i 107 § 1 pkt 6 Kpa.

Rozwijając powyższe należy podnieść, że dokonywanie sprawdzenia danych w rejestrze PESEL bez związku z prowadzoną sprawą może oznaczać, że dostęp ten nie jest realizowany na potrzeby ustawowych zadań uprawnionego podmiotu, których realizacja stanowiła podstawę do przyznania takiemu podmiotowi dostępu do rejestru PESEL w świetle art. 46 ust. 1 ustawy o ewidencji ludności. W tym kontekście wyposażenie aplikacji „A.” w omawianą funkcjonalność przyczyni się także do zapewnienia, że dostęp uprawnionych podmiotów do rejestru PESEL będzie rzeczywiście następował dla celów niezbędnych do realizacji ich ustawowych zadań, a nie w innych celach, niezwiązanych z tymi zadaniami.

Minister Cyfryzacji jako administrator danych przetwarzanych w rejestrze PESEL jest zatem zobowiązany do zastosowania takich środków technicznych i organizacyjnych, które zapewnią, aby wykorzystanie danych pobranych z rejestru PESEL przez uprawnione podmioty następowało w celu realizacji ich ustawowych zadań, a nie w innym celu. W konsekwencji powinien zadbać o bezpieczeństwo tych danych nie tylko na etapie przyznawania dostępu do rejestru PESEL za pomocą urządzeń teletransmisji danych, ale także na etapie pobierania danych osobowych z tego rejestru. Jak już wyżej wskazano, jednym ze środków, który to zapewni, jest wyposażenie aplikacji „A.” w funkcjonalność umożliwiającą podawanie uzasadnienia dla dokonywanego sprawdzenia danych w rejestrze PESEL.

Niezrozumiałe jest ponadto kwestionowanie przez pełnomocnika Ministra Cyfryzacji skuteczności rozwiązania polegającego na wyposażeniu aplikacji „A.” w omawianą funkcjonalność, skoro do tej pory jej nie wdrożono. Brak badań w tym zakresie nie może również uzasadniać braku działań Ministra Cyfryzacji w celu zwiększenia poziomu bezpieczeństwa dla danych osobowych przetwarzanych w ramach rejestru PESEL.

Należy także nadmienić, że Minister Cyfryzacji w piśmie z 28 sierpnia 2017 r., nr […], stanowiącym odpowiedź na zawiadomienie o wszczęciu postępowania administracyjnego, pomimo przedstawienia wątpliwości co do takiego rozwiązania, poinformował o tym, iż przedmiotowa funkcjonalność zostanie wdrożona w aplikacji „A.”.

Budzi zatem zdziwienie wynikająca z wniosku o ponowne rozpatrzenie sprawy zmiana stanowiska przez Ministra Cyfryzacji w tym zakresie.

W świetle przedstawionych wyżej argumentów należy stwierdzić, że nakaz zawarty w pkt 3 decyzji Generalnego Inspektora z 12 września 2017 r., nr DIS/DEC-1110/17/68986, został sformułowany z uwzględnieniem ustalonego w toku kontroli stanu faktycznego i obowiązujących w tym zakresie przepisów prawa. Ustalenia dotyczące aplikacji „A.” i braku funkcjonalności umożliwiającej podawanie uzasadnienia dla dokonywanego sprawdzenia danych w rejestrze PESEL, potwierdzone kontrolami przeprowadzonymi w Ministerstwie Cyfryzacji oraz u wybranych

komorników sądowych, w sposób jednoznaczny pozwalają przyjąć, że doszło do naruszenia art. 36 ust. 1 ustawy o ochronie danych osobowych w związku z niezapewnieniem przez Ministra Cyfryzacji odpowiedniej do zagrożeń ochrony danych osobowych przetwarzanych w ramach rejestru PESEL. Wobec powyższego, nieuzasadniony jest zarzut pełnomocnika Ministra Cyfryzacji o naruszeniu art. 7 Kpa.

W tym stanie prawnym i faktycznym Generalny Inspektor Ochrony Danych Osobowych rozstrzygnął jak w sentencji.

Decyzja jest ostateczna. Strona 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.).