RZECZNIK PRAW OBYWATELSKICH

Warszawa, 29-04-2021 r.

VII.520.6.2020.MKS

Pan
Jan Nowak
Prezes Urzędu Ochrony Danych Osobowych
ePUAP

Szanowny Panie Prezesie,

do Rzecznika Praw Obywatelskich wpływają skargi pracowników inspekcji sanitarnej, dotyczące funkcjonowania systemu SEPIS pod kątem bezpieczeństwa ich danych osobowych. Jak wynika z treści skarg, pracownicy zostali zobowiązani do korzystania z systemu SEPIS przez Profil Zaufany, który w ich ocenie ma charakter prywatny. W ocenie Rzecznika przedstawione w skargach obywateli wątpliwości co do bezpieczeństwa ich danych osobowych, w związku z posługiwaniem się przez nich Profilem Zaufanym w celach służbowych, wydają się uzasadnione, wiążą się bowiem m.in. z ujawnieniem nr PESEL pracowników. Analogiczna zaś sprawa dotycząca stosowania podpisu elektronicznego i związane z tym ujawnianie numeru PESEL pracowników sądów była przedmiotem analizy Rzecznika Praw Obywatelskich i Prezesa UODO. Dlatego też Rzecznik postanowił zwrócić się do Prezesa Urzędu Ochrony Danych Osobowych o zajęcie stanowiska w przedstawionej sprawie.

Rzecznik w pierwszej kolejności wystąpił do Głównego Inspektora Sanitarnego (GIS) z prośbą o informacje w tej sprawie. Z odpowiedzi GIS z dnia 22 marca 2021 r. wynika, że „PZ pozwala użytkownikowi na potwierdzenie tożsamości w systemach teleinformatycznych administracji publicznej bez względu na to czy posiadacz wykorzystuje go w celach prywatnych, czy też wykorzystuje go w celu wykonywania obowiązków pracowniczych (podobnie jak ma to miejsce w przypadku dokumentów stwierdzających

Biuro Rzecznika Praw Obywatelskich
al. Solidarności 77
00-090 Warszawa

Tel. centr. (+48 22) 55 17 700
Infolinia obywatelska 800 676 676
biurorzecznika@brpo.gov.pl
www.rpo.gov.pl

tożsamość, tj. dowodu osobistego lub paszportu w stosunkach tradycyjnych)". Ponadto GIS wskazał, że „w sytuacji gdy w podmiocie publicznym wdrożony jest system teleinformatyczny, za pośrednictwem którego pracownicy danego podmiotu będą wykonywać swoje obowiązki służbowe, a do zalogowania się w tym systemie konieczne jest dysponowanie profilem zaufanym, stosowny obowiązek po stronie pracowników można wywodzić z art. 20a ust. 1 pkt 1 ustawy o informatyzacji" (w załączeniu uprzejmie przesyłam kopię korespondencji RPO z GIS).

Nadesłane wyjaśnienia nie rozwiały wątpliwości Rzecznika. Należy bowiem zauważyć, jak dodatkowo wskazał GIS, że „pracownicy PIS wykorzystują system SEPIS m. in.: do przyjmowania zgłoszeń od obywateli, nakładania kwarantann i izolacji czy też edycji danych związanych z ogniskami epidemii". W konsekwencji należy uznać, że profil zaufany może służyć zarówno do zalogowania się do systemu SEPIS (w celu zidentyfikowania pracownika), jak i do podpisywania dokumentów w imieniu organu (np. przy wydawaniu decyzji). Wiąże się to zatem z ujawnieniem danych osobowych pracownika, w tym nr PESEL w sytuacji podpisu profilem zaufanym.

W tym miejscu pragnę przypomnieć stanowisko Prezesa Urzędu Ochrony Danych Osobowych podzielające wątpliwości Rzecznika w sprawie dotyczącej ujawniania danych identyfikacyjnych pracowników sądowych w pismach urzędowych opatrzonych podpisem elektronicznym (pismo PUODO z dnia 22 maja 2019 r. nr ZSOŚS ZSOŚS.027.37.2019/39374). W ocenie Prezesa UODO, „numer PESEL w rozumieniu art. 87 RODO jest (…) krajowym numerem identyfikacyjnym, którego przetwarzanie powinno odbywać się z zachowaniem odpowiednich zabezpieczeń praw i wolności osoby, której dane dotyczą, przewidzianych w RODO. Wskazany numer PESEL w sposób unikalny identyfikuje daną osobę i pozwala na ustalenie szeregu dodatkowych informacji takich jak płeć, czy wiek tej osoby. Z uwagi na swoją unikalność numer PESEL bywa wykorzystywany również do uwierzytelniania osoby (niestety często w sposób nieprawidłowy, grożący chociażby tzw. *kradzieżą tożsamości*). Przetwarzanie numeru PESEL bez wyraźnie określonej podstawy prawnej i zachowania odpowiednich zasad bezpieczeństwa może stwarzać różnego rodzaju zagrożenia w sferze ochrony danych osobowych".

Wątpliwości Rzecznika budzi również sposób autoryzacji podczas logowania do Profilu Zaufanego, który polega albo na odebraniu sms-ów z hasłem, wysłanych na prywatny telefon, albo w przypadku powiązania Profilu Zaufanego z bankiem – na weryfikacji zgodnej z polityką banku, tj. podanie smsa albo przesłanie hasła, np. kodu jednorazowego z karty kodów. Taki sposób autoryzacji tej usługi, powiązany ze sferą prywatną pracownika, powoduje, że dane osobowe przetwarzane w ramach systemu SEPIS nie są wystarczająco chronione. Należy bowiem zauważyć, że do konta czy telefonu prywatnego pracownika mogą mieć dostęp inne osoby (bliskie) – taką możliwość stwarza chociażby praca zdalna – co może narazić prywatność w wypadku danych dotyczących zdrowia przetwarzanych przez pracowników.

Ponadto, w ocenie RPO, jak słusznie wskazują Skarżący, pracodawca nie może wymagać założenia Profilu Zaufanego przez pracownika. Nie można tym samym zgodzić się z przyjętą przez Państwowego Powiatowego Inspektora Sanitarnego w m. st. Warszawa interpretacją przepisów Kodeksu pracy, zgodnie z którą „podstawą prawną uprawniającą pracodawcę do nałożenia na pracowników Powiatowej Stacji Sanitarno-Epidemiologicznej w m.st. Warszawie wymogu założenia profilu zaufanego w związku z koniecznością zastosowania tego rozwiązania do logowania do SEPIS jest art. 22 § 1 w zw. z art. 100 § 1 Kodeksu pracy” (pismo z dnia 28 listopada 2021 r. będące odpowiedzią na wystąpienie RPO w załączeniu). Brak jest bowiem konkretnego przepisu prawa mogącego być podstawą żądania przez pracodawcę założenia profilu zaufanego przez pracownika i wykorzystywania go w celach służbowych. Tym samym wykonywanie takiego polecenia pracodawcy powinno być dobrowolne, za zgodą pracownika. Brak zgody, lub jej wycofanie, nie może zaś być podstawą niekorzystnego traktowania osoby ubiegającej się o zatrudnienie lub pracownika, a także nie może powodować wobec nich jakichkolwiek negatywnych konsekwencji, zwłaszcza nie może stanowić przyczyny uzasadniającej odmowę zatrudnienia, wypowiedzenie umowy o pracę lub jej rozwiązanie bez wypowiedzenia przez pracodawcę (22^{1a} § 2 Kodeksu pracy).

Niezrozumiałe są również wyjaśnienia GIS odnoszące się kwestii nieudostępnienia procedur dotyczących bezpieczeństwa danych systemu SEPIS, które jak wskazuje GIS „mają charakter niejawny i są w posiadaniu Kancelarii Prezesa Rady Ministrów”.

W ocenie Rzecznika powyższe okoliczności dotyczące wykorzystywania profilu zaufanego w celach zawodowych, tak jak w przypadku pracowników inspekcji sanitarnej do pracy w systemie SEPIS, budzą wątpliwości z punktu widzenia prawa do prywatności i ochrony danych osobowych wyrażonych w 47 i art. 51 ust. 2 Konstytucji RP – gdyż władze publiczne nie mogą pozyskiwać, gromadzić i udostępniać innych informacji o obywatelach niż niezbędne w demokratycznym państwie prawnym. Ponadto przetwarzanie danych osobowych powinno odbywać się z poszanowaniem zasad zawartych w art. 5 ust. 1 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (Dz.U UE L. 119.1 ze sprost.), w szczególności zasady minimalizacji danych.

Mając powyższe na względzie, działając na podstawie art. 12 pkt 2 ustawy z dnia 15 lipca 1987 r. o Rzeczniku Praw Obywatelskich (Dz. U. z 2020 r. poz. 627), zwracam się do Pana Prezesa z prośbą o zbadanie niniejszej sprawy w kontekście wskazanego wyżej stanowiska GIS, a także przedstawionych wątpliwości Rzecznika. Proszę o poinformowanie RPO o dokonanych ustaleniach i stanowisku Pana Prezesa.

Zał. 5

Z poważaniem
Stanisław Trociuk
Zastępca Rzecznika Praw Obywatelskich
/-podpisano elektronicznie/