

GENERALNY INSPEKTOR
OCHRONY DANYCH
OSOBOWYCH

Michał Serzycki

Warszawa, dnia 24 kwietnia 2008 r

DIS/DEC-254/10616/08
dot. DIS-K-421/146/07

DECYZJA

Na podstawie art. 138 § 1 pkt 1 ustawy z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego (Dz. Ui z 2000 r., Nr 98, poz. 1071 z późn. zm.) oraz art. 12 pkt 2, art. 18 ust. 1 pkt 1 i pkt 6 oraz art. 22 w związku z art. 26 ust. 1 pkt 1 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r., Nr 101, poz. 926 z późn. zm.), po przeprowadzeniu postępowania administracyjnego w sprawie wniosku Y, o ponowne rozpatrzenie sprawy zakończonej decyzją Generalnego Inspektora Ochrony Danych Osobowych z dnia 22 lutego 2008 r. sygn. DIS/DEC-134/4605/08,

utrzymuję w mocy zaskarżoną decyzję w zakresie nakazu usunięcia uchybień w procesie przetwarzania danych poprzez:

- 1) usunięcie danych osobowych obejmujących przetworzone do postaci cyfrowej informacje o charakterystycznych punktach linii papilarnych palców pracowników Y w terminie 14 dni od dnia, w którym niniejsza decyzja stanie się ostateczna,**
- 2) zaprzestania zbierania danych osobowych obejmujących przetworzone do postaci cyfrowej informacje o charakterystycznych punktach linii papilarnych palców pracowników Y w terminie od dnia, w którym niniejsza decyzja stanie się ostateczna.**

Uzasadnienie

W dniu 22 lutego 2008 r. Generalny Inspektor Ochrony Danych Osobowych wydał decyzję sygn. DIS/DEC-134/4605/08, nakazującą Y, zwanej dalej także Spółką, usunięcie uchybień w procesie przetwarzania danych osobowych poprzez:

- 1) usunięcie danych osobowych obejmujących przetworzone do postaci cyfrowej informacje o charakterystycznych punktach linii papilarnych palców pracowników Y w terminie 14 dni od dnia, w którym decyzja stanie się ostateczna,
- 2) zaprzestanie zbierania danych osobowych obejmujących przetworzone do postaci cyfrowej informacje o charakterystycznych punktach linii papilarnych palców pracowników Y w terminie od dnia, w którym decyzja stanie się ostateczna,
- 3) opracowanie i wdrożenie polityki bezpieczeństwa w terminie 14 dni od dnia, w którym decyzja stanie się ostateczna,
- 4) opracowanie i wdrożenie instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w terminie 14 dni od dnia, w którym decyzja stanie się ostateczna.

W dniu 11 marca 2008 r. do Biura Generalnego Inspektora Ochrony Danych Osobowych wpłynął, złożony w terminie, Y reprezentowanej przez Pana P, Dyrektora ds. Kadr i Płac oraz Spraw Ogólnych w Y działającego na mocy pełnomocnictwa z dnia 15 stycznia 2008 r. udzielonego przez Prezesa Zarządu Spółki, o ponowne rozpatrzenie sprawy zakończonej decyzją Generalnego Inspektora Ochrony Danych Osobowych z dnia 22 lutego 2008 r. sygn. DIS/DEC-134/4605/08 i zmianę przedmiotowej decyzji w pkt. 1.1 oraz 1.2, a także umorzenie w tym zakresie postępowania jako bezprzedmiotowego. Ww. decyzji zarzucono błędną interpretację i zastosowanie art. 22¹ Kodeksu pracy w związku z art. 6 ustawy o ochronie danych osobowych oraz niezastosowanie art. 23 ust. 1 ustawy.

We wniosku o ponowne rozpatrzenie sprawy strona wskazała ponadto m. in., iż:

- 1) decyzja jest nieprawidłowa w zakresie nakazania Spółce usunięcia danych osobowych obejmujących przetworzone do postaci cyfrowej informacje o charakterystycznych punktach linii papilarnych palców pracowników Y oraz zaprzestania zbierania danych osobowych obejmujących przetworzone do postaci cyfrowej informacje o charakterystycznych punktach linii papilarnych palców pracowników Y,

2) pracodawca nie może „żądać” od pracownika innych informacji niż wymienione w art. 22¹ Kodeksu pracy lub w przepisach szczególnych, a pracownik nie ma „obowiązku” podania takich informacji; dotyczy to również danych biometrycznych; pracodawca może zawsze „ubiegać się”, „zwracać się do pracownika z prośbą” o ich pozyskanie, zaś pracownik, do którego pracodawca zwrócił się o takie informacje, nie ma obowiązku ich podania, ale ma taką „możliwość”,

3) wszyscy pracownicy, od których pobrano linie papilarne, wyrazili na to zgodę wskazując ściśle, w jakim zakresie godzą się na przetwarzanie danych; pracodawca uprzednio pouczył tych pracowników, że podanie danych ma charakter dobrowolny; pracownicy, którzy nie wyrazili zgody, korzystają z innych sposobów rejestracji wejść i wyjść,

4) wbrew informacji zawartej w pouczeniu decyzji wydanej przez Generalnego Inspektora Ochrony Danych Osobowych, decyzja nie ma charakteru decyzji ostatecznej w rozumieniu art. 16 Kpa, w związku z czym strona nie ma prawnego obowiązku jej wykonania, w przypadku złożenia wniosku o ponowne rozpatrzenie sprawy.

5) Wniosek o ponowne rozpatrzenie sprawy nie obejmuje pozostałych nakazów decyzji z dnia 22 lutego 2008 r., sygn. DIS/DEC-134/4605/08, tj. opracowania i wdrożenia polityki bezpieczeństwa oraz instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w terminie 14 dni od dnia, w którym decyzja stanie się ostateczna.

W dniu 3 kwietnia 2008 r. Generalny Inspektor Ochrony Danych Osobowych wydał z urzędu postanowienie sygn. DIS/POST-102/8547/08, w którym sprostował omyłkę pisarską w decyzji z dnia 22 lutego 2008 r., sygn. DIS/DEC-134/4605/08, poprzez zmianę numeracji podpunktów sentencji decyzji, tj. zastąpienie cyfry „2” cyfrą „3” w numeracji podpunktu dotyczącego opracowania polityki bezpieczeństwa oraz cyfry „3” cyfrą „4” w numeracji podpunktu dotyczącego opracowania i wdrożenia instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych. Na ww. postanowienie strona nie wniosła zażalenia. Generalny Inspektor Ochrony Danych Osobowych zważył co następuje: Stosownie do art. 26 ust. 1 pkt 1 ustawy o ochronie danych osobowych, administrator przetwarzający dane powinien dołożyć szczególnej staranności w celu ochrony interesów osób, których dane dotyczą, a w szczególności jest obowiązany zapewnić, aby dane te były przetwarzane zgodnie z prawem. Zgodnie z art. 22¹ § 1 ustawy z dnia 26 czerwca 1974 r. Kodeks pracy (tekst jednolity: Dz. U. z 1998 r. Nr 21, poz. 94 z późn. zm.) pracodawca ma prawo żądać od osoby ubiegającej się o zatrudnienie podania danych osobowych obejmujących: imię (imiona) i nazwisko, imiona rodziców, datę urodzenia, miejsce zamieszkania (adres do korespondencji), wykształcenie, przebieg dotychczasowego zatrudnienia, natomiast w myśl art. 22¹ pracodawca ma prawo żądać od pracownika niezależnie od danych, o których mowa w § 1, także: innych danych osobowych pracownika, a także imion i nazwisk oraz dat urodzenia dzieci pracownika, jeżeli

podanie takich danych jest konieczne ze względu na korzystanie przez pracownika ze szczególnych uprawnień przewidzianych w prawie pracy, numeru PESEL pracownika nadanego przez Rządowe Centrum Informatyczne Powszechnego Elektronicznego Systemu Ewidencji Ludności (RCI PESEL), zaś stosownie do art. 22¹ § 4 pracodawca może żądać podania innych danych osobowych niż określone w § 1 i 2, jeżeli obowiązek ich podania wynika z odrębnych przepisów.

Zgodnie z art. 23 ust. 1 ustawy przetwarzanie danych jest dopuszczalne tylko wtedy, gdy: 1) osoba, której dane dotyczą, wyrazi na to zgodę, chyba że chodzi o usunięcie dotyczących jej danych, 2) jest to niezbędne dla zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa, 3) jest to konieczne do realizacji umowy, gdy osoba, której dane dotyczą, jest jej stroną lub gdy jest to niezbędne do podjęcia działań przed zawarciem umowy na żądanie osoby, której dane dotyczą, 4) jest niezbędne do wykonania określonych prawem zadań realizowanych dla dobra publicznego, 5) jest to niezbędne dla wypełnienia prawnie usprawiedliwionych celów realizowanych przez administratorów danych albo odbiorców danych, a przetwarzanie nie narusza praw i wolności osoby, której dane dotyczą.

W myśl art. 6 ust. 1 ustawy, za dane osobowe uważa się wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. Osobą możliwą do zidentyfikowania jest osoba, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności przez powołanie się na numer identyfikacyjny albo jeden lub kilka specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne.

W toku postępowania ustalono, że w dniu 2 marca 2007 r. Spółka zawarła umowę z S, której przedmiotem jest wdrożenie systemu telewizji dozorowanej CCTV oraz systemu kontroli dostępu na terenie Spółki. W ramach tej umowy S zobowiązała się, między innymi do sprzedaży, instalacji i serwisowania czytników linii papilarnych. W maju 2007 r. zostało zainstalowanych piętnaście czytników linii papilarnych przy poszczególnych wejściach do budynku Spółki, w którym znajdują się pomieszczenia biurowe oraz fabryka.

Ewidencja czasu pracy w Spółce odbywa się zarówno przy użyciu kart radiowych oraz rejestracji za pomocą ww. czytników linii papilarnych. Pracownik może wybrać sposób rejestracji. Jednocześnie, każdy pracownik posiada kartę radiową w celu dostępu do pomieszczeń objętych systemem kontroli dostępu - w ramach nadanych uprawnień.

Dane biometryczne w postaci odcisków palców są zbierane na podstawie zgody wyrażonej przez pracownika w postaci pisemnego oświadczenia o następującej treści: „Ja niżej podpisany wyrażam zgodę na pobranie przez Y wzoru moich linii papilarnych

w celu wprowadzenia ich do bazy danych osób uprawnionych do wejścia i wyjścia na teren firmy Y oraz do rozliczania czasu pracy".

System rejestracji czasu pracy obejmuje czytniki kart radiowych oraz czytniki linii papilarnych wraz z oprogramowaniem służącym do pozyskiwania linii papilarnych oraz do rejestracji wejść i wyjść w oparciu o rejestrowane linie papilarne. Linie papilarne pobierane są z palców dłoni poprzez służący do tego czytnik. Czytnik skanuje obraz linii papilarnych nie zachowując ich obrazu w pamięci. Z informacji uzyskanych od dostawcy (S) wynika, że czytnik przesyła obraz do oprogramowania o nazwie „...”, które przetwarza obraz linii papilarnych na zapis cyfrowy (kod w postaci ciągu cyfr), na podstawie dwunastu charakterystycznych punktów zeskanowanych linii. Obraz linii papilarnych oraz ww. punktów nie jest zapisywany.

Na serwerze zainstalowana jest usługa służąca do komunikacji z terminalami (czytnikami służącymi do rejestracji wejść i wyjść za pomocą linii papilarnych) oraz czytnikiem do pobierania danych biometrycznych. Informacja dotycząca każdego pracownika zapisywana jest w osobnym pliku w określonym miejscu na serwerze. Dodatkowo, w pliku tym zapisywane jest: imię i nazwisko osoby, której linie papilarne zeskanowano, numer identyfikacyjny (ID) danego wpisu oraz obszar, w którym znajdują się czytniki, z których może korzystać ten pracownik. Stosowany jest system, zgodnie z którym nadawany jest taki sam numer Card ID, jaki figuruje na karcie, którą posługuje się pracownik (od czasu, zanim wprowadzono system kontroli dostępu za pomocą linii papilarnych). Następnie dane są przesyłane z serwera do poszczególnych czytników linii papilarnych służących do ewidencji wejść i wyjść. Dane przesyłane z serwera obejmują numer ID oraz kod w postaci ciągu cyfr.

Biorąc za podstawę definicję danych osobowych sformułowaną w wyżej powołanym art. 6 ustawy o ochronie danych osobowych, należy uznać, że dane pracowników Spółki pozyskane przez pracodawcę, przetworzone do postaci zapisu cyfrowego, stanowią dane osobowe w rozumieniu powołanego przepisu. W wyniku zestawienia kodu cyfrowego zarejestrowanego w systemie informatycznym z palcem pracownika przyłożonym do urządzenia skanującego, a także pozostałymi informacjami, możliwa jest identyfikacja tej osoby.

Na podstawie ustalonego stanu faktycznego, w oparciu o obowiązujące przepisy prawa wydając decyzję z dnia 22 lutego 2008 r. sygn. DIS/DEC-134/4605/08, Generalny Inspektor stwierdził, że przetwarzanie danych osobowych pracowników w zakresie ww. kodów cyfrowych odbywa się bez podstawy prawnej. Stosownie bowiem do art. 22¹ Kodeksu pracy, pracodawca może żądać od pracownika podania danych tylko w takim zakresie, jaki został wskazany w powołanym przepisie. Przepis art. 22¹ § 1 i § 2 Kodeksu pracy dopuszcza żądanie od pracownika podania wyłącznie danych zaliczonych do określonego w tym przepisie katalogu informacji. Pozostałe

informacje o pracowniku ustawodawca uznał generalnie za niedostępne dla pracodawcy. Wprowadził jednak jeden wyjątek (art. 22¹ § 4 k.p.) tj. pracodawca może żądać podania innych danych osobowych niż określone w art. 22¹ § 1 i § 2 k.p., jeżeli obowiązek ich podania wynika z odrębnych przepisów. Do przedmiotowego stanu faktycznego nie znajdują zastosowania przepisy prawa, które zezwalałyby na przetwarzanie w celu prowadzenia ewidencji czasu pracy innych danych osobowych, niż wymienione w art. 22¹ § 1 i § 2 k.p. Jednocześnie organ podkreślił, że powołane przepisy Kodeksu pracy zostały wprowadzone w ramach dostosowania wskazanego aktu prawnego do art. 51 ust. 1 Konstytucji Rzeczypospolitej Polskiej, zgodnie z którym nikt nie może być obowiązany inaczej niż na podstawie ustawy do ujawnienia informacji dotyczących jego osoby. A zatem zdaniem Generalnego Inspektora, złożenie przez pracownika oświadczenia, którego treścią jest wyrażenie zgody na rejestrację czasu pracy za pomocą czytnika palców, nie stanowi przesłanki legalizującej przetwarzanie danych osobowych pracowników wbrew argumentacji przedstawionej przez Stronę we wniosku o ponowne rozpatrzenie sprawy. Za niezasadne należy uznać również twierdzenie Spółki, iż organ wykazał się nieznajomością znaczenia w języku . polskim słowa „żądać”. Ustawodawca przyznając pracodawcy prawo do żądania od pracownika jedynie danych wskazanych w art. 22¹ § 1 i § 2 k.p. (poza wyjątkami wskazanymi w art. 22¹ § 4 k.p.), tym samym zezwolił na przetwarzanie danych wyłącznie w tym zakresie i wyłączył możliwość przetwarzania danych na podstawie innych przesłanek, w tym przewidzianych w art. 23 ust. 1 ustawy o ochronie danych osobowych. Wobec powyższego, za błędny należy uznać również zarzut Strony, iż rozstrzygając przedmiotową sprawę organ nie zastosował art. 23 ust. 1 ustawy. Konsekwencją bowiem uznania, że doszło do naruszenia art. 26 ust. 1 pkt 1 ustawy poprzez przetwarzanie danych osobowych niezgodnie z prawem, jest stwierdzenie, iż w przedmiotowym stanie faktycznym nie zachodzi żadna z przesłanek przetwarzania danych osobowych, wymieniona w art. 23 ust. 1 ustawy.

Niniejszym należy odnieść się również do wyrażonego przez Spółkę stwierdzenia, iż decyzja Generalnego Inspektora z dnia 22 lutego 2008 r. sygn. DIS/DEC-134/4605/08 nie ma charakteru decyzji ostatecznej. Stosownie do art. 21 ust. 2 ustawy o ochronie danych osobowych strona, wobec której Generalny Inspektor Ochrony Danych Osobowych wydał decyzję, może zwrócić się z wnioskiem o ponowne rozpatrzenie sprawy. Również z art. 127 § 3 Kpa wynika, że od decyzji wydanej w pierwszej instancji przez ministra nie służy odwołanie, jednakże strona niezadowolona z decyzji może zwrócić się do tego organu z wnioskiem o ponowne rozpatrzenie sprawy; do wniosku tego stosuje się odpowiednio przepisy dotyczące odwołań od decyzji. Pojęcie „ministra” zostało zdefiniowane w art. 5 § 2 pkt 4 Kpa. W myśl art. 16 § 1 Kpa decyzje, od których nie służy odwołanie w administracyjnym toku instancji, są ostateczne. Decyzja wydana przez Generalnego Inspektora jest zatem ostateczna z chwilą jej wydania. Mimo, iż wniosek o ponowne rozpatrzenie

sprawy stanowi odrębny środek zaskarżenia, odpowiednio stosuje się do niego, jak wynika z powołanego wyżej przepisu, przepisy o odwołaniu. Należy zatem uznać, iż poza przepisami, które ze swej istoty nie mogą zostać zastosowane do omawianego wniosku, pozostałe przepisy odnoszące się do odwołań mają do niego zastosowanie. W szczególności należy wskazać zasadę wyrażoną w art. 130 § 1 Kpa, zgodnie z którą przed upływem terminu do wniesienia odwołania decyzja nie ulega wykonaniu. Za oczywiste należy zatem uznać, iż mimo przysługiwania decyzji Generalnego Inspektora waloru ostateczności, do czasu wniesienia wniosku o ponowne rozpatrzenie sprawy nie powinna zostać ona wykonana przez stronę. Dopiero upływ terminu do wniesienia środka zaskarżenia rodzi po stronie adresata decyzji obowiązek wykonania tego aktu administracyjnego. Jeżeli natomiast strona w terminie wystąpi z wnioskiem o ponowne rozpatrzenie sprawy, w myśl art. 130 § 2 Kpa wykonanie decyzji zostaje wstrzymane.

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