GENERALNY INSPEKTOR
OCHRONY DANYCH
OSOBOWYCH
Michał Serzycki

Warszawa, 22 lutego 2008 r.

DIS/DEC- *134/4605/08*
Dot. DIS-K-421/146/07

DECYZJA

Na podstawie art. 104 § 1 i art. 105 § 1 ustawy z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego (Dz. U. z 2000 r., Nr 98, poz. 1071 z późn. zm.), art. 12 pkt 2, art. 18 ust. 1 pkt 1 i pkt 6, art. -22 w związku z art. 26 ust. 1 pkt 1, art. 36 ust. 2 i ust. 3 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r., Nr 101, poz. 926 z późn. zm.) oraz § 3 ust. 1, ust. 2 i ust. 3 rozporządzenia 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), po przeprowadzeniu postępowania administracyjnego w sprawie przetwarzania danych osobowych przez Y,

I. Nakazuję Y usunięcie 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. **Zaprzestanie 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.

2. **Opracowanie i wdrożenie polityki bezpieczeństwa w terminie 14 dni od dnia,** w którym **niniejsza decyzja stanie się ostateczna.**
3. **Opracowanie i wdrożenie instrukcji zarządzania systemem informatycznym służącym** do **przetwarzania danych osobowych w terminie 14 dni od dnia, w którym niniejsza decyzja stanie się ostateczna.**

II. W pozostałym zakresie postępowanie umarzam.

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

_____ Inspektorzy upoważnieni przez Generalnego Inspektora Ochrony Danych Osobowych, Przeprowadzili w Y, zwanej dalej Spółką, kontrolę zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych (sygn. kontroli DIS-K), tj. ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r., Nr 101, poz. 926 z późn. zm.) 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. W toku kontroli odebrano od pracowników Spółki 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 Prezesa Zarządu Y.

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

1. Przetwarzaniu bez podstawy prawnej danych osobowych obejmujących przetworzone do postaci cyfrowej (kod w postaci ciągu cyfr) informacje o charakterystycznych punktach linii papilarnych palców pracowników Spółki.
2. Braku polityki bezpieczeństwa oraz instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.
3. Niewyznaczeniu administratora bezpieczeństwa informacji.

W związku z powyższym, w dniu 10 stycznia 2008 r. Generalny Inspektor Ochrony Danych Osobowych wszczął z urzędu postępowanie administracyjne w niniejszej sprawie w celu wyjaśnienia okoliczności sprawy (sygn. pisma DIS-K).

W odpowiedzi na zawiadomienie o wszczęciu postępowania administracyjnego Pełnomocnik Spółki pismem z dnia 21 stycznia 2008 r. złożył wyjaśnienia, w których poinformował, że:

1. Pracodawca nie może żądać od pracownika innych informacji niż wymienione w art. 22 ustawy z dnia 26 czerwca 1974 r. Kodeks pracy (tekst jednolity: Dz. U. z 1998 r. Nr 21, poz. 94 z późn. zm.) lub w przepisach szczególnych, a pracownik nie ma obowiązku podawania takich informacji. Dotyczy to również danych biometrycznych stanowiących dane osobowe w rozumieniu ustawy o ochronie danych osobowych. Jednakże pracodawca może ubiegać się o pozyskanie ww. danych, a pracownik ma możliwość ich podania, pod warunkiem wyrażenia przez pracownika zgody na przetwarzanie takich danych oraz zapewnienia przez pracodawcę należytej ochrony dóbr osobistych i godności pracownika.
2. Dokumentacja, na którą składa się polityka bezpieczeństwa i instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych zostanie opracowana w terminie 14 dni.
3. W Spółce wyznaczony został administrator bezpieczeństwa informacji.

Do pisma z dnia 21 stycznia 2008 r. załączono zarządzenie Dyrektora Kadr i Płac oraz Spraw Ogólnych w Spółce z dnia 18 stycznia 2008 r. w sprawie powołania i upoważnienia do wykonywania zadań administratora danych osobowych przetwarzanych w Y oraz wyznaczenia administratora bezpieczeństwa informacji, jako dowód potwierdzający wyznaczenie w Spółce administratora bezpieczeństwa informacji.

Po zapoznaniu się z całością materiału dowodowego zebranego w sprawie 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. $22^{:}$ § 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. 22^{1} § 2 pracodawca ma prawo żądać od pracownika podania, 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. 22^1 § 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 w 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 urządzania skanującego, a także pozostałymi informacjami, możliwa jest identyfikacja tej osoby.

Na podstawie ustalonego stanu faktycznego, w oparciu o obowiązujące przepisy prawa należy stwierdzić, że przetwarzanie danych osobowych pracowników w zakresie ww. kodów cyfrowych odbywa się bez podstawy prawnej. Stosownie bowiem do art. 22^1 Kodeksu pracy, pracodawca może żądać od pracownika podania danych tylko w takim zakresie, jaki został wskazany w powołanym przepisie. Przepis art. 22^1 § 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. 22^1 § 4 k.p.) tj. pracodawca może żądać podania innych danych osobowych niż określone w art. 22^1 § 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. 22^1 § 1 i § 2 k.p. Jednocześnie należy podkreślić, 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.

W świetle powyższych rozważań, złożenie przez pracownika oświadczenia, którego treścią jest wyrażenie zgody na rejestrację czasu pracy za pomocą czytnika palców, nie stanowi przesłania legalizującej przetwarzanie danych osobowych pracowników.

Zgodnie z art. 36 ust. 2 ustawy, administrator danych prowadzi dokumentację opisującą sposób przetwarzania danych oraz środki, o których mowa w ust. 1. W myśl § 3 ust. 1 rozporządzenia, na dokumentację, o której mowa w § 1 pkt 1 rozporządzenia, składa się polityka bezpieczeństwa i instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych. Zgodnie z § 3 ust. 2, dokumentację, o której mowa w § 1 pkt 1 rozporządzenia, prowadzi się w formie pisemnej, stosownie do § 3 ust. 3 rozporządzenia, dokumentację, o której mowa w § 1 pkt 1 rozporządzenia, wdraża administrator danych.

W toku czynności kontrolnych ustalono, że Spółka nie prowadzi dokumentacji opisującej sposób przetwarzania danych oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną tj. polityki bezpieczeństwa i instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.

Generalny Inspektor uwzględniając wyjaśnienia Spółki dotyczące podjęcia działań zmierzających do opracowania polityki bezpieczeństwa i instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych wyznaczył czternastodniowy termin wykonania niniejszej decyzji.

Stosowanie do art. 105 § 1 Kodeksu postępowania administracyjnego, gdy postępowanie z jakiejkolwiek przyczyny stało się bezprzedmiotowe, organ administracji publicznej wydaje decyzję o jego umorzeniu. Przesłanką umorzenia postępowania na podstawie art. 105 § 1 k.p.a jest bezprzedmiotowość postępowania „z jakiejkolwiek przyczyny", czyli z każdej przyczyny powodującej brak jednego z elementów materialnoprawnego stosunku prawnego w odniesieniu do jego strony podmiotowej lub przedmiotowej (wyrok NSA z 21 stycznia 1999 r. SA/Szl029/97).

W toku postępowania usunięte zostało uchybienie w procesie przetwarzania danych osobowych stanowiące przedmiot postępowania poprzez wyznaczenie w Spółce administratora bezpieczeństwa informacji, dlatego w tym zakresie należało je umorzyć.

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

GENERALNY INSPEKTOR
OCHRONY DANYCH OSOBOWYCH
Michał Serzycki