



**GENERALNY INSPEKTOR  
OCHRONY DANYCH  
OSOBOWYCH**

*Michał Serzycki*

**Warszawa, dnia 25 lutego 2010 r.**

**DOLiS-035-115/10**

**p.o. Dyrektor  
Zespołu Szkół [...] w S.**

**proszę o dostosowanie procesu przetwarzania danych osobowych do zasad wynikających z przepisów ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. 2002 r. Nr 101, poz. 926 z późn. zm.).**

W nawiązaniu do dotychczasowej korespondencji, pozostającej w związku wprowadzeniem w Zespole Szkół [...] z siedzibą w S. przy ul. [...], zwanym dalej Zespołem Szkół, elektronicznego systemu kontroli dostępu na teren Zespołu Szkół, który odczytuje (skanuje) obraz linii papilarnych nauczycieli, pracowników i uczniów Zespołu Szkół, proszę o uwzględnienie przepisów ustawy o ochronie danych osobowych w procesie przetwarzania przez Zespół Szkół danych osobowych ww. osób.

Zgodnie z brzmieniem art. 7 ustawy z dnia 2 kwietnia 1997 r. Konstytucja Rzeczypospolitej Polskiej (Dz. U. 1997 r. Nr 78, poz. 483 ze zm.), organy władzy publicznej działają na podstawie i w granicach prawa (zasada legalizmu). Przepis ten implikuje, iż wszelkie działania ograniczające konstytucyjne wolności i prawa osobiste człowieka i obywatela, w tym również prawo do ochrony danych osobowych, powinny znajdować ustawową podstawę prawną. Prawo do ochrony prawnej życia prywatnego zostało zagwarantowane w treści art. 47 Konstytucji Rzeczypospolitej Polskiej, zaś poszczególne uprawnienia, składające się na treść tego prawa – w innych przepisach konstytucyjnych. W myśl zaś art. 51 ust. 1 Konstytucji Rzeczypospolitej Polskiej, nikt nie może być obowiązany inaczej niż na podstawie ustawy do ujawniania informacji dotyczących jego osoby. Przepis ten nie określa w sposób jednoznaczny podmiotu zobowiązanego do realizacji prawa w nim zagwarantowanego. Oznacza to, że wymieniony przepis konstytucyjny dotyczy wszelkich przypadków, w których jednostka zobowiązana zostaje do ujawniania informacji o sobie innym podmiotom (instytucjom, osobom). Art. 31 ust. 3 Konstytucji Rzeczypospolitej Polskiej stanowi, iż ograniczenia

w zakresie korzystania z konstytucyjnych wolności i praw mogą być ustanawiane tylko w ustawie i tylko wtedy, gdy są konieczne w demokratycznym państwie dla jego bezpieczeństwa lub porządku publicznego, bądź dla ochrony środowiska, zdrowia i moralności publicznej, albo wolności i praw innych osób. Ograniczenia te nie mogą naruszać istoty wolności i praw.

Podmioty przetwarzające dane osobowe są obowiązane do stosowania przepisów ustawy o ochronie danych osobowych na każdym etapie przetwarzania tych danych, o ile przepisy innych aktów prawnych nie określają w sposób szczególny procesu przetwarzania danych osobowych. Przez przetwarzanie danych osobowych rozumieć należy jakiejkolwiek operacje wykonywane na danych osobowych (art. 7 pkt 2 ustawy o ochronie danych osobowych). W świetle zaś ustawowej definicji, za dane osobowe uznaje się zarówno takie informacje, które pozwalają bezpośrednio na określenie tożsamości konkretnej osoby, jak również takie, które nie pozwalają na jej natychmiastową identyfikację, są jednakże przy pewnym nakładzie kosztów, czasu lub działań, wystarczające do jej ustalenia. Nie stanowią natomiast danych osobowych takie informacje, na podstawie których nie jest możliwe zidentyfikowanie osoby oraz takie, na podstawie których wprowadzić można byłoby ją zidentyfikować, lecz wiązałoby się to z nadmiernymi kosztami, czasem lub działaniami.

Dane biometryczne określonej osoby, takie jak np. jej linie papilarne, czy obraz tęczówki oka, niewątpliwie można uznać za dane osobowe, jako pozwalające na ustalenie tożsamości osoby w sposób pewny. Z racji ich wyłącznej przynależności do danej osoby, dane biometryczne stanowią swego rodzaju „identyfikator” osoby fizycznej. W tym miejscu zasadnym jest odwołanie się do opinii niezależnego organu konsultacyjnego Unii Europejskiej, jakim jest Grupa Robocza do spraw ochrony osób wobec przetwarzania danych osobowych, powołana na mocy art. 29 Dyrektywy 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r., przyjętej w dniu 1 sierpnia 2003 r., pt. „Dokument Roboczy w sprawie biometrii” (12168/02/FR GT 80). Jak wskazano w przedmiotowej opinii cyt.: „ (...) szybki rozwój technologii biometrycznych jak i coraz powszechniejsze ich stosowanie w ostatnich latach wymagają uważnej analizy z punktu widzenia ochrony danych. Powszechne i niekontrolowane posługiwanie się biometrią wzbudza niepokój z punktu widzenia ochrony wolności i fundamentalnych praw człowieka. (...) Szczególne zaniepokojenie związane z danymi biometrycznymi wzbudza ryzyko zmniejszenia wrażliwości ludzi spowodowane coraz większą powszechnością używania tych danych na konsekwencje, jakie przetwarzanie ich danych może mieć w ich życiu codziennym. Na przykład, posługiwanie się biometrią w bibliotekach może zmniejszyć świadomość dzieci co do zagrożeń związanych z ochroną danych, które mogą później mieć dla nich poważne konsekwencje w życiu. (...) dane biometryczne zawsze mogą być uważane za „dane dotyczące osoby fizycznej”, ponieważ dotyczy to danych ze swej natury dotyczących określonej osoby”.

Zakres danych osobowych, jakie pracodawca może gromadzić w związku z zatrudnieniem, został szczegółowo określony w przepisach art. 22<sup>1</sup> ustawy z dnia 26 czerwca 1974 r. Kodeks pracy (tekst jednolity: Dz. U. 1998 r. Nr 21, poz. 94 z późn. zm.). Art. 22<sup>1</sup> § 5 ustawy Kodeks pracy stanowi,

iż w zakresie nieuregulowanym w § 1-4 do danych osobowych, o których mowa w tych przepisach, stosuje się przepisy o ochronie danych osobowych. W obowiązującym w Polsce porządku prawnym brak jest przepisów powszechnie obowiązujących, odnoszących się do szerokiej kategorii podmiotów, na podstawie których pracodawca mógłby żądać udostępnienia przez pracowników ich danych biometrycznych, do których należą m.in. linie papilarne. Brak też przepisów prawa, które dają podstawę do przetwarzania takich danych uczniów.

Pozyskiwanie odcisków palców, jak również porównywanie odwzorowania punktów charakterystycznych palca przez czytniki linii papilarnych z zapisanymi na nich danymi, w celu ich identyfikacji w związku z wprowadzeniem systemu dokonującego na ich podstawie kontroli dostępu do budynku (np. szkoły) oceniane jest przez organ do spraw ochrony danych osobowych jako prowadzące do naruszenia zasady adekwatności przetwarzania danych, o której mowa w art. 26 ust. 1 pkt 3 ustawy o ochronie danych osobowych. Zgodnie z tym przepisem, administrator danych przetwarzający dane powinien dołożyć szczególnej staranności w celu ochrony interesów osób, których dane dotyczą, a w szczególności jest obowiązany zapewnić, aby dane te były merytorycznie poprawne i adekwatne w stosunku do celów, w jakich są przetwarzane. W wyroku z dnia 1 grudnia 2005 r. Wojewódzki Sąd Administracyjny (sygn. II SA/Wa 917/2005) orzekł, iż cyt.: *„Adekwatność danych w stosunku do celu ich przetwarzania powinna być rozumiana jako równowaga pomiędzy uprawnieniem osoby do dysponowania swymi danymi a interesem administratora danych. Równowaga będzie zachowana, jeżeli administrator zażąda danych tylko w takim zakresie, w jakim jest to niezbędne do wypełnienia celu, w jakim dane są przez niego przetwarzane”*. Stwierdzenie to implikuje wniosek, iż administrator danych nie może przetwarzać danych w zakresie szerszym niż niezbędny dla osiągnięcia zamierzonego celu, jak również danych o większym, niż uzasadniony tym celem stopniu szczegółowości. Gromadzenie odcisków palców nauczycieli, pracowników i uczniów Zespołu Szkół zdecydowanie nie jest adekwatne do celu ich przetwarzania, tj. zapewnienia im bezpieczeństwa na terenie Zespołu Szkół. Ponadto nie bez znaczenia jest, iż pozyskiwanie przedmiotowych danych prowadzi do zbyt daleko idącej ingerencji w prywatność ww. osób. Zespół Szkół – jako placówka oświatowa - jest obowiązany czuwać nie tylko nad takimi dobrami uczniów, jak np. ich bezpieczeństwo, ale także obowiązany jest dbać, aby nie dochodziło do sytuacji mogących spowodować niezgodne z prawem przetwarzanie danych osobowych uczniów uczęszczających do Zespołu Szkół. Pozyskiwanie jednakże obrazów linii papilarnych uczniów, w celu zapewnienia im poczucia bezpieczeństwa, jest ingerencją w sferę ich konstytucyjnej wolności, a także może prowadzić do zlekceważenia rangi ważności danych biometrycznych, jakimi są linie papilarne, w świadomości młodych osób wkraczających w dorosłe życie, nie znajdującą uzasadnienia w obowiązujących przepisach prawa wynikających np. z ustawy o systemie oświaty.

Wskazać również należy na wyrok Naczelnego Sądu Administracyjnego w Warszawie z dnia 1 grudnia 2009 r. (sygn. akt I OSK 249/09), w którym NSA orzekł, iż cyt.: *„w przyjętym przez Grupę*

*(Grupa Robocza Artykułu 29 ds. ochrony danych osobowych) w dniu 1 sierpnia 2003 r. dokumencie roboczym w sprawie Biometrii przyjęto jako niezbędną zasadę proporcjonalności i legalności. Oznacza to, że ryzyko naruszenia swobód i fundamentalnych praw obywatelskich musi być proporcjonalne do celu, któremu służy. Skoro zasada proporcjonalności wyrażona w art. 26 ust. 1 pkt 3 ustawy o ochronie danych osobowych jest głównym kryterium przy podejmowaniu decyzji dotyczących przetwarzania danych biometrycznych, to stwierdzić należy, że wykorzystanie danych biometrycznych do kontroli czasu pracy pracowników (...) jest nieproporcjonalne do zamierzonego celu ich przetwarzania". Sąd przyjął zatem w tej sprawie, że pozyskiwanie danych biometrycznych jest nadmierną ingerencją w prywatność człowieka.*

Na marginesie należy wskazać, iż odmiennie należałoby rozpatrywać ewentualne pozyskiwanie danych biometrycznych celem zapewnienia bezpieczeństwa jedynie w szczególnie istotnych strefach na terenie Zespołu Szkół, a w konsekwencji, gdy przebywanie w innych częściach strefy ich pracy i nauki nie byłoby uwarunkowane pozyskiwaniem i przetwarzaniem danych osobowych o charakterze biometrycznym.

Argumentacji wskazanej w piśmie Pani Dyrektor z dnia [...] stycznia 2010 r. nie można zatem uznać za słuszną i trafną.

Konkludując, zasadnym jest odstąpienie od przetwarzania odcisków palców (cyfrowego obrazu linii papilarnych) pracowników, nauczycieli i uczniów Zespołu Szkół w celu zapewnienia im bezpieczeństwa, w szczególności, gdy możliwe jest stosownie innych technik autoryzacji wejść/wyjść, nie ingerujących tak głęboko w prywatność – prawo zagwarantowane konstytucyjnie.

Proszę zatem Panią Dyrektor o podjęcie stosownych działań, mających na celu dostosowanie procesu przetwarzania danych osobowych pracowników, nauczycieli i uczniów Zespołu Szkół do powszechnie obowiązujących przepisów prawa, w szczególności zaś o uwzględnienie przepisów ustawy Kodeks pracy oraz ustawy o ochronie danych osobowych, oraz o poinformowanie Generalnego Inspektora Ochrony Danych Osobowych o działaniach podjętych w przedmiotowej sprawie.