



**GENERALNY INSPEKTOR  
OCHRONY DANYCH  
OSOBOWYCH**

*Michał Serzycki*

Warszawa, dnia 9 stycznia 2009 r.

DIS/DEC-15/615/09

dot. [...]

**D E C Y Z J A**

Na podstawie art. 104 § 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 art. 22 w związku z art. 24 ust. 1 pkt 3 i pkt 4, art. 36 ust. 2, art. 37, art. 38, art. 39, art. 40 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, § 7 ust. 1 pkt 1 i pkt 2 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 Miejskie Przedsiębiorstwo Komunikacyjne Sp. z o.o.,

**Nakazuję Miejskiemu Przedsiębiorstwu Komunikacyjnemu Sp. z o.o., usunięcie uchybień w procesie przetwarzania danych osobowych, poprzez:**

**1. Dopelnianie obowiązku informacyjnego, o którym mowa w art. 24 ust. 1 pkt 3 i pkt 4 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.), tj. w zakresie informowania osób, którym zostały wydane legitymacje**

przewoźnika o prawie dostępu do treści swoich danych oraz ich poprawiania, a także obowiązku podania danych, w terminie 3 miesięcy od dnia, w którym niniejsza decyzja stanie się ostateczna.

2. Zgłoszenie do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych zbioru danych osób, którym wydawane są legitymacje przewoźnika, w terminie 3 miesięcy od dnia, w którym niniejsza decyzja stanie się ostateczna.

3. Opracowanie w formie pisemnej dokumentacji opisującej sposób przetwarzania danych osobowych 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, w terminie 3 miesięcy od dnia, w którym niniejsza decyzja stanie się ostateczna.

4. Opracowanie upoważnień do przetwarzania danych osobowych, w terminie 3 miesięcy od dnia, w którym niniejsza decyzja stanie się ostateczna.

5. Spowodowanie, by system informatyczny o nazwie „A”, w którym przetwarzane są dane osobowe osób ubiegających się o wydanie legitymacji dla każdej osoby, której dane osobowe są przetwarzane w tym systemie informatycznym, odnotowywał datę pierwszego wprowadzenia danych do systemu oraz identyfikator użytkownika wprowadzającego dane osobowe do systemu, w terminie 3 miesięcy od dnia, w którym niniejsza decyzja stanie się ostateczna.

6. Opracowanie ewidencji osób upoważnionych do przetwarzania danych osobowych, w terminie 3 miesięcy od dnia, w którym niniejsza decyzja stanie się ostateczna.

### **Uzasadnienie**

Inspektorzy, upoważnieni przez Generalnego Inspektora Ochrony Danych Osobowych przeprowadzili kontrolę w Miejskim Przedsiębiorstwie Komunikacyjnym Sp. z o.o., zwanej dalej Spółką, w celu ustalenia zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych sygn. [...], 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, oraz 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 Spółki.

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

1. Niedopełnieniu obowiązku informacyjnego (art. 24 ust. 1 pkt 3 i pkt 4 ustawy).
2. Niezgłoszeniu do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych zbioru danych osób, którym wydawane są legitymacje przewoźnika (art. 40 ustawy).
3. Nieopracowaniu w formie pisemnej dokumentacji opisującej sposób przetwarzania danych osobowych 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 (art. 36 ust. 2 ustawy w związku z § 3 rozporządzenia).
4. Nieopracowaniu upoważnień do przetwarzania danych (art. 37 ustawy).
5. Niezapewnieniu, aby system informatyczny o nazwie „A” dla każdej osoby, której dane osobowe są przetwarzane w tym systemie informatycznym, odnotowywał, datę pierwszego wprowadzenia danych do systemu oraz identyfikator użytkownika wprowadzającego dane osobowe do systemu (§ 7 ust. 1 pkt 1 i pkt 2 rozporządzenia).
6. Nieopracowaniu ewidencji osób upoważnionych do przetwarzania danych osobowych (art. 39 ustawy).

W piśmie z dnia [...] grudnia 2008 r. sygn. [...], stanowiącym zawiadomienie o wszczęciu postępowania administracyjnego w przedmiotowej sprawie, Spółka została poinformowana o prawie czynnego udziału w każdym stadium postępowania, a przed wydaniem decyzji wypowiedzenia się co do zebranych dowodów i materiałów oraz zgłoszonych żądań.

W odpowiedzi na zawiadomienie o wszczęciu postępowania administracyjnego Prezes Zarządu Spółki, pismem z dnia [...] grudnia 2008 r. złożył wyjaśnienia, w których poinformował, iż uchybienia stwierdzone w trakcie kontroli nie zostały przez Spółkę w pełni usunięte. Jednocześnie ww. wskazał trzy miesięczny termin na usunięcie uchybień wskazanych w pkt 1, pkt 2, pkt 3, pkt 4 i pkt 6 zawiadomienia o wszczęciu postępowania administracyjnego, natomiast odnośnie usunięcia uchybienia wskazanego w pkt 5 (dotyczącego systemu informatycznego o nazwie „A”) wskazał 2009 r. W powołanym piśmie Prezes Zarządu Spółki zwrócił się także z prośbą o nie wydawanie decyzji administracyjnej przed upływem wyżej wskazanych terminów.

Po zapoznaniu się z całością materiału dowodowego zebranego w sprawie Generalny Inspektor Ochrony Danych Osobowych zważył co następuje:

Zgodnie z art. 24 ust. 1 pkt 3 i pkt 4 ustawy, w przypadku zbierania danych osobowych od osoby, której one dotyczą, administrator danych jest obowiązany poinformować tę osobę o prawie dostępu do treści swoich danych oraz ich poprawiania oraz dobrowolności albo obowiązku podania danych, a jeżeli taki obowiązek istnieje, o jego podstawie prawnej.

Jak ustalono w toku kontroli obowiązek informacyjny w zakresie art. 24 ust. 1 pkt 1 i pkt 2 ustawy, realizowany jest wobec osób, którym są wydawane legitymacje przewoźnika na stronie internetowej Przewoźnika oraz w środkach komunikacji zbiorowej. Natomiast obowiązek informacyjny odnośnie art. 24 ust. 1 pkt 3 oraz pkt 4, tj. informacji o prawie dostępu do treści swoich danych oraz ich poprawiania, a także obowiązku podania danych, nie jest przez Spółkę realizowany.

Zgodnie z art. 40 ustawy, administrator danych jest obowiązany zgłosić zbiór danych do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych. Przez zbiór danych osobowych, zgodnie z art. 7 pkt 1 ustawy, rozumie się każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie.

Jak wynika z ustaleń kontroli zbiór danych osobowych osób, którym są wydawane legitymacje przewoźnika, prowadzony jest w systemie informatycznym. Jednocześnie w trakcie oględzin systemu informatycznego o nazwie „A” w module „B”, ustalono, iż w module tym rejestrowane są dane w zakresie: nazwisko, imię, data urodzenia, nr PESEL, gmina, adres (miejscowość, ulica, nr domu, nr mieszkania), grupa (podstawa do wydania legitymacji); nr legitymacji oraz data wydania legitymacji.

Biorąc pod uwagę wskazane wyżej okoliczności, należy stwierdzić, iż przetwarzane w systemie informatycznym o nazwie „A” dane osobowe tworzą zbiór danych osobowych, o którym mowa w art. 7 pkt 1 ustawy. Dane zawarte w ww. systemie informatycznym dostępne są według określonych kryteriów, tj. w szczególności według imienia i nazwiska.

Mając powyższe na uwadze uznać należy, iż Spółka przetwarza dane osobowe osób, którym wydawane są legitymacje przewoźnika. Nie zachodzi przy tym żadna z okoliczności wskazanych w art. 43 ust. 1 ustawy, zwalniających Spółkę z obowiązku zgłoszenia do rejestracji powyższego zbioru danych.

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, 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, prowadzi

się w formie pisemnej. Natomiast, zgodnie z ust. 3, dokumentację, o której mowa w § 1 pkt 1, wdraża administrator danych. W zakresie zawartości merytorycznej, wymienione wyżej dokumenty powinny spełniać warunki określone w § 4 i § 5 rozporządzenia.

W toku kontroli ustalono, iż w Spółce nie jest prowadzona dokumentacja opisująca sposób przetwarzania danych osobowych, tj. polityka bezpieczeństwa i instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.

Zgodnie z art. 37 ustawy, do przetwarzania danych mogą być dopuszczone wyłącznie osoby posiadające upoważnienie nadane przez administratora danych.

W toku czynności kontrolnych ustalono, że w Spółce do przetwarzania danych dopuszczone zostały osoby nie posiadające upoważnienia nadanego przez administratora danych.

Zgodnie z art. 38 ustawy, administrator danych jest obowiązany zapewnić kontrolę nad tym, jakie dane osobowe, kiedy i przez kogo zostały do zbioru wprowadzone oraz komu są przekazywane.

Natomiast zgodnie z § 7 ust. 1 pkt 1 i pkt 2 rozporządzenia, dla każdej osoby, której dane osobowe są przetwarzane w systemie informatycznym - z wyjątkiem systemów służących do przetwarzania danych osobowych ograniczonych wyłącznie do edycji tekstu w celu udostępnienia go na piśmie - system ten zapewnia odnotowanie daty pierwszego wprowadzenia danych do systemu; identyfikator użytkownika wprowadzającego dane osobowe do systemu, chyba że dostęp do systemu informatycznego i przetwarzanych w nim danych posiada wyłącznie jedna osoba.

W toku czynności kontrolnych ustalono, że system informatyczny o nazwie „A”, w którym przetwarzane są dane osobowe osób ubiegających się o wydanie legitymacji uprawniającej do korzystania z biletów ulgowych nie zapewnia odnotowania daty pierwszego wprowadzenia danych do systemu oraz identyfikator użytkownika wprowadzającego dane osobowe do systemu.

Zgodnie art. 39 ustawy, administrator danych prowadzi ewidencję osób upoważnionych do przetwarzania danych osobowych, która powinna zawierać: 1) imię i nazwisko osoby upoważnionej, 2) datę nadania i ustania oraz zakres upoważnienia do przetwarzania danych osobowych, 3) identyfikator, jeżeli dane są przetwarzane w systemie informatycznym.

W toku czynności kontrolnych ustalono, że w Spółce, nie jest prowadzona ewidencja osób upoważnionych do przetwarzania danych, która spełnia wymagania określone w art. 39 ustawy.

Jednocześnie należy wskazać, że Generalny Inspektor Ochrony Danych Osobowych nie mógł przychylić się do prośby Prezesa Zarządu Spółki w kwestii dotyczącej „nie wydawania decyzji w przedmiotowej sprawie do czasu usunięcia wszystkich uchybień”.

Podjęcie działań w celu usunięcia uchybień nie stanowi podstawy do uznania, iż przywrócony został stan zgodny z prawem. Nie przedstawiono dowodów potwierdzających, iż powyższe

uchybień zostały usunięte. Jednak zważywszy na podjęte działania w tym zakresie wyznaczono 3 miesięczny termin na usunięcie przedmiotowych uchybień.

Mając powyższe na uwadze, w tym stanie prawnym i faktycznym, Generalny Inspektor Ochrony Danych Osobowych rozstrzygnął, jak w sentencji.

Decyzja jest ostateczna. Na podstawie art. 21 ust. 1 ustawy o ochronie danych osobowych oraz art. 129 § 2 Kodeksu postępowania administracyjnego, strona niezadowolona z niniejszej decyzji może zwrócić się do Generalnego Inspektora Ochrony Danych Osobowych (adres: ul. Stawki 2, 00-193 Warszawa) z wnioskiem o ponowne rozpatrzenie sprawy, w terminie 14 dni od dnia doręczenia niniejszej decyzji.