



**GENERALNY INSPEKTOR  
OCHRONY DANYCH  
OSOBOWYCH**

*Michał Serzycki*

Warszawa, dnia 3 grudnia 2009 r.

DIS/DEC-1205/44971, 44985/09

Dot. DIS-K-421/131/09

**D E C Y Z J A**

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, art. 22 i art. 31 ust. 5 w związku z art. 36 ust. 2 i ust. 3, art. 37 i art. 39 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r., Nr 101, poz. 926 z późn. zm.), § 3 ust. 1, § 4 pkt 1 – 5, § 5 pkt 3 i pkt 6 – 8 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 urzędnicy i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100, poz. 1024), oraz częścią A pkt IV ust. 2 załącznika do ww. rozporządzenia, po przeprowadzeniu postępowania administracyjnego w sprawie przetwarzania danych osobowych przez Z, jako podmiot, któremu administrator danych, tj. Prezydent Miasta, na podstawie umowy, o której mowa w art. 31 ust. 1 ustawy o ochronie danych osobowych powierzył przetwarzanie danych osobowych w związku z funkcjonowaniem karty miejskiej,

**I. Nakazuję Z usunięcie uchybień w procesie przetwarzania danych osobowych poprzez:**

- 1. Uzupełnienie wykazu zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych, stanowiącego element polityki bezpieczeństwa, o informacje dotyczące systemu informatycznego o nazwie „S”, służącego do przetwarzania danych osobowych w związku z funkcjonowaniem karty miejskiej, w terminie 30 dni od dnia, w którym niniejsza decyzja stanie się ostateczna.**

- 2. Uzupełnienie instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych o procedury rozpoczęcia, zawieszenia i zakończenia pracy, przeznaczone dla użytkowników systemów informatycznych o nazwach „S” i „V” oraz o informacje dotyczące sposobu realizacji wymogów, o których mowa w § 7 ust. 1 pkt 4 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), w terminie 30 dni od dnia, w którym niniejsza decyzja stanie się ostateczna.**
- 3. Zapewnienie, aby zmiana hasła służącego do uwierzytelnienia użytkownika w systemie informatycznym o nazwie „S” następowała nie rzadziej niż co 30 dni, w terminie 3 miesięcy 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 Z, zwanej dalej Spółką, kontrolę zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych (sygn. DIS-K-421/131/09), tj. ustawą z dnia 29 sierpnia 1997r. 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 podpisanym przez osoby upoważnione do reprezentowania Spółki.

Na podstawie zgromadzonego materiału dowodowego ustalono, że Prezydent Miasta, jako administrator danych, na podstawie umowy zawartej w dniu 9 grudnia 2008 r., powierzył Spółce przetwarzanie danych osobowych. Ww. umowa stanowi umowę powierzenia przetwarzania danych osobowych, o której mowa w art. 31 ust. 1 ustawy. Stosownie do art. 31 ust. 3 ustawy, podmiot, o którym mowa w ust. 1 (podmiot, któremu powierzono przetwarzanie danych osobowych) jest obowiązany przed rozpoczęciem przetwarzania danych podjąć środki zabezpieczające zbiór danych, o których mowa w art. 36 - 39, oraz spełnić wymagania określone w przepisach, o których mowa

w art. 39a. W zakresie przestrzegania tych przepisów podmiot ponosi odpowiedzialność jak administrator danych. Natomiast w myśl art. 31 ust. 4 ustawy, w przypadkach, o których mowa w ust. 1 - 3, odpowiedzialność za przestrzeganie przepisów niniejszej ustawy spoczywa na administratorze danych, co nie wyłącza odpowiedzialności podmiotu, który zawarł umowę, za przetwarzanie danych niezgodnie z tą umową.

Ustalenia dokonane w toku kontroli wskazują, że w procesie przetwarzania danych osobowych Spółka, jako podmiot, któremu administrator danych powierzył przetwarzanie danych, naruszyła przepisy o ochronie danych osobowych. Uchybienia te polegały na:

1. Niezawarcu w dokumentacji opisującej sposób przetwarzania danych oraz środki, o których mowa w art. 36 ust. 1 ustawy, wszystkich wymaganych informacji jakie powinna zawierać polityka bezpieczeństwa oraz instrukcja zarządzania systemem informatycznym (art. 36 ust. 2 ustawy w związku z § 4 pkt 1 – 5 i § 5 pkt 3 i pkt 6 – 8 rozporządzenia).
2. Niewyznaczeniu administratora bezpieczeństwa informacji (art. 36 ust. 3 ustawy).
3. Nienadaniu osobom przetwarzającym dane osobowe upoważnień do przetwarzania ww. danych (art. 37 ustawy).
4. Niezawarcu w ewidencji osób upoważnionych do przetwarzania danych osobowych wszystkich osób upoważnionych do przetwarzania ww. danych, jak również daty nadania i ustania upoważnienia do przetwarzania danych osobowych (art. 39 ustawy).
5. Niezabezpieczeniu za pomocą hasła zmienianego nie rzadziej niż co 30 dni systemów informatycznych o nazwach „S” i „V” (część A pkt IV ust. 2 załącznika do rozporządzenia).

W związku z powyższym w dniu 23 września 2009 r. Generalny Inspektor Ochrony Danych Osobowych wszczął z urzędu postępowanie administracyjne w niniejszej sprawie w celu wyjaśnienia okoliczności sprawy (sygn. DIS-K-421/131/09/34706).

W odpowiedzi na zawiadomienie o wszczęciu postępowania administracyjnego pełnomocnik Spółki w piśmie z dnia 6 października 2009 r. złożył wyjaśnienia, w których poinformował między innymi, że:

1. Prezydent Miasta w związku z funkcjonowaniem karty miejskiej nie powierzył Spółce przetwarzania danych osobowych.
2. Miasto nie udostępnia Spółce żadnych danych osobowych przetwarzanych w systemie informatycznym o nazwie „S”, a Spółka ma jedynie dostęp do modułów ww. systemu zawierających raporty i wykresy, które nie są danymi osobowymi.
3. Spółka ma dostęp do numerów kart miejskich, nie ma jednak możliwości identyfikacji osoby fizycznej według numeru karty miejskiej.
4. Urząd Miejski odmówił przekazania Spółce danych osobowych pasażerów.

5. Spółka usunęła uchybienia w procesie przetwarzania danych osobowych dotyczące: dokumentacji opisującej sposób przetwarzania danych oraz środki, o których mowa w art. 36 ust. 1 ustawy, wyznaczenia administratora bezpieczeństwa informacji oraz posiadania przez pracowników Spółki upoważnień do przetwarzania danych osobowych.
6. Dostęp do systemu informatycznego o nazwie „E”, którego poprawna nazwa brzmi „S” został przez operatora systemu (E) przyznany tylko na jedno stanowisko pracy. Dostęp Spółki do ww. systemu ograniczony jest do modułu „Raporty i wykresy” i nie obejmuje dostępu do danych osobowych. Spółka nie ma wpływu na funkcjonalność ww. systemu ponieważ z E nie łączy jej żadna umowa, a zakres dostępu do wskazanego systemu wynika z konieczności realizacji usługi przewozów w komunikacji miejskiej.
7. Spółka usunęła uchybienia dotyczące braków w ewidencji osób upoważnionych do przetwarzania danych osobowych.
8. Zgodnie z opracowaną w Spółce „Polityką stosowania haseł” hasła do systemu informatycznego o nazwie „V” zmieniane będą co 30 dni.

Do pisma pełnomocnika Spółki z dnia 6 października 2009 r., jako dowody mające potwierdzić przesłane wyjaśnienia, załączono: kserokopię opisu systemu karty miejskiej, kserokopię pisma Urzędu Miejskiego z dnia 3 czerwca 2009 r., kopię korespondencji e-mail z dnia 28 września 2009 r. z załączonym do niej projektem porozumienia w sprawie reklamacji wadliwych kart, kserokopię polityki bezpieczeństwa i instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, kserokopię polityki stosowania haseł dostępu do systemów informatycznych, kserokopię opisu struktur i granic obszarów przetwarzania danych osobowych, kserokopię uchwały w sprawie wyznaczenia administratora bezpieczeństwa informacji, kserokopie oświadczeń dotyczących potwierdzenia zapoznania się z polityką bezpieczeństwa i instrukcją zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, kserokopie aneksów do zakresów obowiązków pracowników Spółki, kserokopię wykazu osób upoważnionych do przetwarzania danych osobowych w Spółce.

Ponadto, do pisma pełnomocnika Spółki z dnia 24 listopada 2009 r. załączono uaktualniony wykaz osób upoważnionych do przetwarzania danych osobowych w Spółce.

Jednocześnie, dnia 23 września 2009 r. skierowane zostało pismo do administratora danych, tj. do Prezydenta Miasta, informujące o wszczęciu postępowania administracyjnego wobec Spółki (sygn. DIS-K-421/131/09/34710). W odpowiedzi na ww. pismo Prezydent Miasta w piśmie z dnia 4 października 2009 r. złożył wyjaśnienia, w których poinformował między innymi, że Miasto nie upoważniło Spółki do przetwarzania danych osobowych w systemie karty miejskiej i nie przekazało kodów dostępu do przedmiotowego systemu, a jedynie udostępniło Spółce dostęp do zestawień, raportów i wykresów generowanych przez system „S”.

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

Biorąc pod uwagę wyjaśnienia złożone przez Spółkę, jak i przez Prezydenta Miasta, zgodnie z którymi administrator danych, tj. Prezydent Miasta, nie powierzył Spółce przetwarzania danych osobowych w związku z funkcjonowaniem karty miejskiej należy wskazać, iż powyższe wyjaśnienia nie zasługują na uwzględnienie. W toku kontroli ustalono, że Spółka posiada dostęp do systemu informatycznego o nazwie „S”, w którym przetwarzane są dane osobowe w związku z funkcjonowaniem systemu karty miejskiej. Omawiany dostęp do danych wynika z umowy, o której mowa w art. 31 ust. 1 ustawy, zawartej przez Spółkę z administratorem danych, tj. z Prezydentem Miasta T, w dniu 9 grudnia 2008 r. Postanowienia ww. umowy wskazują wprost, iż administrator danych zapewni Spółce dostęp do danych przetwarzanych w związku z funkcjonowaniem karty miejskiej. W toku przeprowadzonej kontroli ustalono, że Spółka posiada między innymi dostęp do danych dotyczących historii użycia karty, na przykład takich jak: nr karty, nr autobusu, nr linii, daty i czasu użycia karty, nr przystanku, nazwy przystanku. Mając na uwadze, iż zgodnie z art. 6 ust. 1 ustawy, za dane osobowe uważa się wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej, a osobą możliwą do zidentyfikowania jest osoba, której tożsamość można określić bezpośrednio lub pośrednio, należy uznać, że numer karty miejskiej, jak i dane dotyczące historii jej użycia, są danymi osobowymi w rozumieniu ustawy o ochronie danych osobowych.

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, zwana dalej „instrukcją”. Stosownie do § 4 pkt 2 rozporządzenia, polityka bezpieczeństwa, o której mowa w § 3 ust. 1, zawiera w szczególności wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych. Natomiast w myśl § 5 pkt 3 i pkt 7 rozporządzenia, instrukcja, o której mowa w § 3 ust. 1, zawiera w szczególności procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu oraz sposób realizacji wymogów, o których mowa w § 7 ust. 1 pkt 4.

Na podstawie analizy przesłanych przez Spółkę wyjaśnień oraz dołączonych do nich dokumentów ustalono, iż nie wszystkie stwierdzone w toku kontroli uchybienia dotyczące polityki bezpieczeństwa i instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych zostały usunięte, tj. w polityce bezpieczeństwa nie

wskazano w wykazie zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych informacji dotyczących systemu informatycznego o nazwie „S”, natomiast w instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych nie wskazano procedur rozpoczęcia, zawieszenia

i zakończenia pracy przeznaczonych dla użytkowników systemu oraz informacji dotyczących sposobu realizacji wymogów, o których mowa w § 7 ust. 1 pkt 4 rozporządzenia.

Zgodnie z częścią A pkt IV ust. 2 załącznika do rozporządzenia, w przypadku, gdy do uwierzytelniania użytkowników używa się hasła, jego zmiana następuje nie rzadziej, niż co 30 dni.

W toku kontroli ustalono, że hasło do systemu informatycznego o nazwie „S” nie jest zmieniane. Z wyjaśnień złożonych przez Spółkę wynika, iż nie ma ona wpływu na funkcjonalność ww. systemu, ponieważ nie jest jego właścicielem. Należy wskazać, iż powyższe wyjaśnienia nie zasługują na uwzględnienie, gdyż zgodnie z art. 31 ust. 3 ustawy, w zakresie przestrzegania przepisów dotyczących zabezpieczenia przetwarzanych danych osobowych podmiot, któremu powierzono przetwarzanie danych osobowych ponosi odpowiedzialność jak administrator ww. danych. Jednakże, uwzględniając złożone wyjaśnienia, wyznaczono trzymiesięczny termin na usunięcie w tym zakresie uchybień w procesie przetwarzania danych osobowych.

Nie można również zgodzić się z twierdzeniem, iż Spółka nie ma wpływu na funkcjonalność systemu „S”, ponieważ z E nie łączy jej żadna umowa. Należy wskazać, iż dnia 9 grudnia 2009 r. Spółka zawarła umowę, której stroną jest E. Z § 5 pkt 3 powołanej umowy wynika zobowiązanie E do zapewnienia, aby urządzenia i system informatyczny służące do obsługi systemu karty miejskiej spełniały wymagania przepisów dotyczących ochrony danych osobowych. Wobec powyższego należy uznać, iż Spółka ma wpływ na funkcjonalność systemu „S” poprzez egzekwowanie postanowień powołanej umowy.

Ponadto, w niniejszej decyzji uwzględniono wyjaśnienia dotyczące nazwy systemu informatycznego służącego do przetwarzania danych osobowych w związku z funkcjonowaniem systemu karty miejskiej. W toku kontroli pracownicy Spółki składający wyjaśnienia w zakresie ww. systemu posługiwali się nazwą „E” i taka nazwa została użyta w protokole kontroli podpisanym przez osoby uprawnione do reprezentacji Spółki, do którego nie wniesiono uwag i zastrzeżeń. Jednakże, uwzględniając przesłane przez Spółkę wyjaśnienia z dnia 6 października 2009 r., jak również wyjaśnienia administratora danych, tj. Prezydenta Miasta, z dnia 4 października 2009 r., w niniejszej decyzji nazwa „E” została zastąpiona nazwą „S”.

Jednocześnie, na podstawie złożonych przez pełnomocnika Spółki pisemnych wyjaśnień oraz nadesłanych dokumentów, należy stwierdzić, że pozostałe uchybienia w procesie przetwarzania danych osobowych stanowiące przedmiot postępowania zostały usunięte, tj.:

1. Uzupełniono politykę bezpieczeństwa o:

- wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe (§ 4 pkt 1 rozporządzenia),
- opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi (§ 4 pkt 3 rozporządzenia),
- sposób przepływu danych pomiędzy poszczególnymi systemami (§ 4 pkt 4 rozporządzenia),
- określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych (§ 4 pkt 5 rozporządzenia).

2. Uzupełniono instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych o:

- sposób zabezpieczenia systemu informatycznego przed działalnością oprogramowania, o którym mowa w pkt III ppkt 1 załącznika do rozporządzenia (§ 5 pkt 6 rozporządzenia),
- procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych (§ 5 pkt 8 rozporządzenia).

3. Powołano administratora bezpieczeństwa informacji.

4. Pracownikom przetwarzającym dane osobowe nadano upoważnienia do przetwarzania danych.

5. Opracowano ewidencję osób upoważnionych do przetwarzania danych osobowych, która spełnia wymagania określone w art. 39 ustawy.

6. Hasło do systemu informatycznego o nazwie „V” zmieniane jest co 30 dni.

Stosownie do art. 105 § 1 Kodeksu postępowania administracyjnego, gdy postępowanie z jakiegokolwiek 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 jakiegokolwiek 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/Sz1029/97).

Z uwagi na to, iż pozostałe uchybienia będące przedmiotem niniejszego postępowania administracyjnego zostały usunięte, postępowanie należało w tym zakresie umorzyć.

Wobec powyższego, 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.