



**GENERALNY INSPEKTOR
OCHRONY DANYCH
OSOBOWYCH**

dr Wojciech R. Wiewiórowski

Warszawa, dnia 16 września 2011 r.

DIS/DEC-1110/64638/11

Dot. [...]

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 i art. 22 w związku z art. 7 pkt 5, art. 23 ust. 1 pkt 1, art. 26 ust. 1 pkt 1, art. 36 ust. 2, art. 36 ust. 3, art. 40 i art. 41 ust. 2 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r., Nr 101, poz. 926 z późn. zm.) oraz § 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), po przeprowadzeniu postępowania administracyjnego w sprawie przetwarzania danych osobowych przez K. Spółka Akcyjna,

I. Nakazuję K. Spółka Akcyjna, jako administratorowi danych, usunięcie uchybienia w procesie przetwarzania danych osobowych poprzez: wyznaczenie administratora bezpieczeństwa informacji, nadzorującego przestrzeganie zasad ochrony przetwarzanych danych osobowych- w terminie 7 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 kontrolę sygn. akt [...] w K. S.A. (zwanej dalej Spółką), w celu ustalenia zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych, 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 Członka Zarządu Spółki.

Na podstawie całokształtu materiału dowodowego zgromadzonego w sprawie ustalono, iż K. Spółka Akcyjna, jako administrator danych, naruszyła przepisy o ochronie danych osobowych. Stwierdzone uchybienia polegały na:

1. Niezapewnieniu osobom wypełniającym „Wniosek o wydanie Karty [...]” opcjonalności w kwestii *wyrażenia zgody* bądź *nie wyrażenia zgody* na: przetwarzanie ich danych osobowych w celach marketingowych i promocyjnych oraz na przekazywanie ich danych osobowych innym podmiotom; przetwarzanie danych osobowych w celach marketingowych i promocyjnych przez [...] i E. Sp. z o.o. (art. 23 ust. 1 pkt 1 w zw. z art. 7 pkt 5 ustawy).
2. Przetwarzaniu w systemie informatycznym o nazwie „A” (służącym do przetwarzania danych osobowych kibiców [...]) bez podstawy prawnej następujących danych osobowych: nazwiska rodzowego, serii i numeru dowodu osobistego (mimo że w systemie tym jest przetwarzany numer PESEL dotyczący tej osoby), adresu zameldowania, miejsca i daty urodzenia, wzrostu, koloru oczu, daty wydania dowodu osobistego i nazwy organu, który wydał ten dokument, imion rodziców (art. 26 ust. 1 pkt 1 ustawy).
3. Niezawarciu w polityce bezpieczeństwa informacji, o których mowa w § 4 rozporządzenia.
4. Niewyznaczeniu w Spółce administratora bezpieczeństwa informacji, nadzorującego przestrzeganie zasad ochrony przetwarzanych danych osobowych (art. 36 ust. 3 ustawy).
5. Niezgłoszeniu do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych zbioru danych osób, których dane są przetwarzane w celu marketingowym oraz zbioru danych osób objętych monitoringiem (art. 40 ustawy).
6. Niezgłoszeniu Generalnemu Inspektorowi Ochrony Danych Osobowych zmian w zbiorze danych osobowych o nazwie „K” (księga rejestrowa nr [...]) dotyczących zakresu danych przetwarzanych w zbiorze oraz informacji o odbiorcach, którym dane są przekazywane (art. 41 ust. 2 ustawy).

W dniu [...] października 2011 r. Generalny Inspektor Ochrony Danych Osobowych wszczął z urzędu postępowanie administracyjne w niniejszej sprawie w celu wyjaśnienia okoliczności sprawy. Pismem zawiadamiającym o wszczęciu postępowania administracyjnego w przedmiotowej sprawie znak: [...], administrator danych, tj. 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.

Pismem z dnia [...] listopada 2011 r. Członek Zarządu Spółki zwrócił się z wnioskiem o przedłużenie terminu do dnia [...] listopada 2011 r. na złożenie wyjaśnień, zgłoszenie wniosków dowodowych. W dniu [...] grudnia 2011 r. wpłynęło do Biura Generalnego Inspektora Ochrony Danych Osobowych pismo Członka Zarządu Spółki z dnia [...] listopada 2011 r. zawierające wyjaśnienia dotyczące usunięcia uchybień wskazanych w piśmie z dnia [...] października 2011 r. znak: [...].

Ze złożonych wyjaśnień wynika, m. in., iż:

1. W związku z wydaniem Karty [...], Spółka obecnie pozyskuje dane osobowe w następującym zakresie: imię i nazwisko, wizerunek twarzy oraz numer PESEL.
2. Spółka przetwarza dane osobowe [...] jedynie w celu identyfikacji osób uczestniczących w imprezach masowych. Podstawą prawną do przetwarzania danych ww. osób stanowi art. 13 ust. 4 pkt 2 ustawy o bezpieczeństwie imprez masowych. Spółka nie przetwarza danych osobowych kibiców w celach marketingowych i promocyjnych i w związku z tym zmodyfikowany został formularz „Wniosku o wydanie Karty [...]”, poprzez usunięcie z niego klauzul zgody na przetwarzanie danych osobowych w ww. celach.
3. Obecnie w systemie informatycznym o nazwie „A” Spółka nie przetwarza danych osobowych kibiców takich jak: nazwisko rodowe, seria i numer dowodu osobistego, adres zameldowania, miejsce i data urodzenia, wzrost, kolor oczu, data wydania dowodu osobistego i nazwa organu, który wydał ten dokument oraz imion rodziców.
4. Zarządzeniem nr [...] z dnia [...] listopada 2011 r. Prezesa Zarządu Spółki wprowadzone zostały zmiany dotyczące polityki bezpieczeństwa. Obecnie dokument ten zawiera wszystkie niezbędne elementy, o których mowa w § 4 rozporządzenia, tj.: wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe; wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych; opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązań między nimi; sposób przepływu danych pomiędzy poszczególnymi systemami; określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych.

5. W Spółce powołano administratora bezpieczeństwa informacji, poprzez zawarcie umowy na administrację bezpieczeństwem informacji z firmą zewnętrzną.
6. Spółka zgłosiła do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych zbior danych o nazwie „O”.
7. Spółka nie przetwarza danych osobowych kibiców w celach marketingowych i w związku z tym Spółka nie jest zobowiązana do zgłoszenia Generalnemu Inspektorowi Ochrony Danych Osobowych zbioru danych przetwarzanych w tym celu.
8. Na podstawie art. 41 ust. 2 ustawy o ochronie danych osobowych Spółka zgłosiła Generalnemu Inspektorowi Ochrony Danych Osobowych zmiany dotyczące zbioru danych o nazwie „K” (księga rejestrowa nr [...]).

Ponadto, do ww. pisma załączono dowody mające potwierdzić złożone wyjaśnienia w postaci: formularza „Wniosku o wydanie karty [...]”; wydruk z systemu informatycznego o nazwie „A” potwierdzającego zakres danych osobowych przetwarzanych w tym systemie; kopii zgłoszenia do rejestracji zbioru danych o nazwie „O”; kopii zgłoszenia aktualizacji zbioru danych o nazwie „K” (księga rejestrowa nr [...]); kopii Zarządzenia nr [...] z dnia [...] listopada 2011 r. Prezesa Zarządu Spółki w sprawie polityki bezpieczeństwa obowiązującej w Spółce; kopii dokumentu o nazwie „Polityka Bezpieczeństwa Informacji [...]”.

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

Zgodnie z art. 36 ust. 3 ustawy, administrator danych wyznacza administratora bezpieczeństwa informacji, nadzorującego przestrzeganie zasad ochrony, o których mowa w ust. 1, chyba że sam wykonuje te czynności.

W toku kontroli ustalono, iż w Spółce nie został powołany administrator bezpieczeństwa informacji.

Pismem z dnia [...] listopada 2011 r. stanowiącym odpowiedź na zawiadomienie o wszczęciu postępowania administracyjnego Spółka poinformowała, iż w Spółce powołano administratora bezpieczeństwa informacji, poprzez zawarcie umowy na administrację bezpieczeństwem informacji z firmą zewnętrzną. Ze względu na okoliczność, iż do ww. pisma nie załączono dowodu w postaci kopii umowy, o której mowa powyżej, nie można stwierdzić, czy administrator danych prawidłowo wyznaczył administratora bezpieczeństwa informacji, tj. osobę fizyczną, która nadzorować ma w Spółce przestrzeganie zasad ochrony danych osobowych. Bowiem należy wskazać, iż w literaturze przedmiotu, przyjmuje się, że administratorem bezpieczeństwa informacji musi być osoba fizyczna (por. A. Drozd, „Ustawa o ochronie danych

osobowych. Komentarz. Wzory pism i przepisy.”, wydanie 4, str. 264-265; P. Barta i P. Litwiński, „Ustawa o ochronie danych osobowych. Komentarz.”, Warszawa 2009, str. 372).

Ze względu na powyższe nie można uznać, iż został przywrócony stan zgodny z prawem w zakresie, o którym mowa powyżej.

Jednocześnie, na podstawie złożonych przez administratora danych pisemnych wyjaśnień oraz załączonych dowodów należy stwierdzić, że Spółka usunęła pozostałe uchybienia w procesie przetwarzania danych osobowych, tj.:

1. Zmodyfikowany został formularz „Wniosku o wydanie Karty [...]”, który obecnie nie zawiera klauzuli zgody na przetwarzanie danych osobowych w celach marketingowych i promocyjnych (art. 23 ust. 1 ustawy).
2. Zaprzestano przetwarzania w systemie informatycznym o nazwie „A” danych osobowych w następującym zakresie: serii i numeru dowodu osobistego (w przypadku, gdy nie jest przetwarzany numer PESEL dotyczący tej osoby), adresu zameldowania, miejsca i daty urodzenia, wzrostu, koloru oczu, daty wydania dowodu osobistego i nazwy organu, który wydał ten dokument, imion rodziców (art. 26 ust. 1 pkt 1 ustawy).
3. W dokumencie o nazwie „Polityka Bezpieczeństwa Informacji [...]” zawarto informacje dotyczące: wykazu budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe; wykazu zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych; opisu struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązań między nimi; sposobu przepływu danych pomiędzy poszczególnymi systemami; określenia środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych (§ 4 rozporządzenia).
4. Spółka zgłosiła do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych zbiór danych o nazwie „O” (art. 40 ustawy).
5. Spółka nie przetwarza danych osobowych kibiców w celach marketingowych i w związku z tym nie jest zobowiązana do zgłoszenia Generalnemu Inspektorowi Ochrony Danych Osobowych zbioru danych przetwarzanych w tym celu (art. 40 ustawy).
6. Spółka zgłosiła Generalnemu Inspektorowi Ochrony Danych Osobowych zmiany aktualizacyjne dotyczące zbioru danych o nazwie „K” - księga rejestrowa nr [...] (art. 41 ust. 2 ustawy).

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

beprzedmiotowość 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. S.A./Sz1029/97).

W toku postępowania usunięte zostały pozostałe uchybienia w procesie przetwarzania danych osobowych, stanowiące przedmiot postępowania i dlatego należało je umorzyć.

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

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.

W razie niewykonania decyzji w terminie zostanie wobec podmiotu zobowiązanego do jej wykonania wszczęte postępowanie egzekucyjne na podstawie przepisów ustawy z dnia 17 czerwca 1966 r. o postępowaniu egzekucyjnym w administracji (Dz. U. z 2005 r. Nr 229, poz. 1954 z późn. zm.).