



**GENERALNY INSPEKTOR
OCHRONY DANYCH
OSOBOWYCH**

dr Wojciech R. Wiewiórowski

Warszawa, dnia 20 września 2011 r.

DIS/DEC – 816/44889, 44891/11

dot. DIS-K-421/108/11

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, art. 22 w związku z art. 31 ust. 3 i art. 36 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 § 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. z 2004 r., Nr 100, poz. 1024) oraz częścią A pkt IV ust. 3 załącznika do ww. rozporządzenia, po przeprowadzeniu postępowania administracyjnego w sprawie przetwarzania danych osobowych przez spółkę zajmującą się holdingiem nieruchomości, jako podmiotu, któremu wspólnota mieszkaniowa, stosownie do art. 31 ustawy o ochronie danych osobowych, powierzyła przetwarzanie danych osobowych,

nakazuję spółce zajmującej się holdingiem nieruchomości, przywrócenie stanu zgodnego z prawem, poprzez:

- 1. Wyznaczenie administratora bezpieczeństwa informacji, w terminie od dnia, w którym niniejsza decyzja stanie się ostateczna.**
- 2. Uzupełnienie polityki bezpieczeństwa o 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 powiązania między nimi; sposób przepływu danych pomiędzy poszczególnymi systemami; określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych, w terminie miesiąca od dnia, w którym niniejsza decyzja stanie się ostateczna.**
- 3. Wykonywanie kopii zapasowych danych osobowych członków wspólnoty mieszkaniowej przetwarzanych przy użyciu systemu informatycznego o nazwie „XYZ”, w terminie od dnia, w którym niniejsza decyzja stanie się ostateczna.**

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

Inspektorzy upoważnieni przez Generalnego Inspektora Ochrony Danych Osobowych, przeprowadzili kontrolę (sygn. akt DIS-K-421/108/11) w spółce zajmującej się holdingiem nieruchomości (Spółce) w celu ustalenia zgodności przetwarzania danych 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. z 2004 r., Nr 100, poz. 1024) zwanym dalej rozporządzeniem. W toku kontroli odebrano ustne wyjaśnienia od pracowników Spółki, oraz dokonano oględzin pomieszczeń, w których odbywa się przetwarzanie danych osobowych. Stan faktyczny został szczegółowo opisany w protokole kontroli, który został podpisany przez Prezesa i Wiceprezesa Zarządu Spółki.

W toku kontroli DIS-K-421/108/11 ustalono, że Spółka powstała w dniu 22 kwietnia 2011 r. w wyniku połączenia w trybie art. 492 § 1 pkt 2 ustawy z dnia 15 września 2000 r. Kodeks spółek handlowych (Dz. U. Nr 94, poz. 1037 z późn. zm.) sześciu innych Spółek w tym m.in. spółki A i spółki B, stając się następcą prawnym ww. Spółek, przejmując ich wszelkie prawa i obowiązki. Dnia 16 lutego 2011 r. spółka A zawarła ze wspólnotą mieszkaniową, jako administratorem danych w rozumieniu art. 7 pkt 4 ustawy, umowę o administrowanie nieruchomością. W związku z

realizacją tej umowy Spółka przetwarza dane osobowe członków wspólnoty mieszkaniowej, występując w roli podmiotu, o którym mowa w art. 31 ustawy tj. podmiotu, któremu administrator danych powierzył w drodze umowy na piśmie przetwarzanie danych osobowych.

Zgodnie z art. 31 ust. 3 ustawy, podmiot o którym mowa w ust. 1, jest obowiązany przed rozpoczęciem przetwarzania danych podjąć środki zabezpieczające zbiór danych, o których mowa w art. 36-39 ustawy, oraz spełnić wymagania określone w przepisach, o których mowa w art. 39a ustawy. 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.

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

1. Niewyznaczeniu administratora bezpieczeństwa informacji (art. 36 ust. 3 ustawy),
2. Niezawarcia w polityce bezpieczeństwa 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),
3. Niewykonywaniu kopii zapasowych danych osobowych członków wspólnoty mieszkaniowej przetwarzanych przy użyciu systemu informatycznego o nazwie „XYZ” (część A pkt IV ust. 3 załącznika do ww. rozporządzenia).

W związku z powyższym, Generalny Inspektor Ochrony Danych Osobowych wszczął z urzędu postępowanie administracyjne w niniejszej sprawie w celu wyjaśnienia okoliczności sprawy. Pismem z dnia 11 sierpnia 2011 r. zawiadamiającym o wszczęciu postępowania administracyjnego w przedmiotowej sprawie (sygn. DIS-K-421/108/11/38582) 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.

Jednocześnie, w piśmie z dnia 11 sierpnia 2011 r. (sygn. DIS-K-421/108/11/38583) wspólnota mieszkaniowa, jako administrator danych osobowych swoich członków została zawiadomiona o wszczęciu postępowania administracyjnego wobec Spółki, 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 22 sierpnia 2011 r. złożył wyjaśnienia, z których wynika, że:

1. Do dnia 31 sierpnia 2011 r. zostanie w Spółce wyznaczony administrator bezpieczeństwa informacji,
2. Spółka prowadzi prace mające na celu uzupełnienie obowiązującej w Spółce polityki bezpieczeństwa,
3. W Spółce wykonywane są, na nośnikach zewnętrznych, kopie zapasowe danych osobowych członków wspólnoty mieszkaniowej przetwarzanych przy użyciu systemu informatycznego o nazwie „XYZ”.

Do ww. pisma Spółka nie załączyła żadnych dowodów potwierdzających ww. informacje, a także nie przekazała Generalnemu Inspektorowi dowodu potwierdzającego wyznaczenie w Spółce administratora bezpieczeństwa informacji.

Po zapoznaniu się z całością materiału dowodowego zebranego w 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, że w Spółce nie został wyznaczony administrator bezpieczeństwa informacji, a wyjaśnienia Prezesa Zarządu Spółki z dnia 22 sierpnia 2011 r. nie zostały poparte żadnym dowodem potwierdzającym wyznaczenie takiej osoby w Spółce. Z uwagi na powyższe uznać należy, iż ww. uchybienie nie zostało usunięte.

Zgodnie z § 4 rozporządzenia polityka bezpieczeństwa powinna zawierać: 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 powiązania między nimi; sposób przepływu danych pomiędzy poszczególnymi systemami; określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych.

Analiza przedłożonej przez Spółkę w toku kontroli „Polityki bezpieczeństwa” stanowiącej załącznik nr 2 do Uchwały Nr 1/0812/09 Zarządu spółki B z dnia 8 grudnia 2009 r. w sprawie ochrony danych osobowych w Spółce B wykazała, że nie zawiera ona: 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

W odpowiedzi na zawiadomienie o wszczęciu postępowania administracyjnego Spółka pismem z dnia 22 sierpnia 2011 r. poinformowała Generalnego Inspektora jedynie o tym, że trwają obecnie prace mające na celu zmianę polityki bezpieczeństwa przedłożonej przez Spółkę w toku czynności kontrolnych. Z uwagi na powyższe należy stwierdzić, że ww. uchybienie nie zostało przez Spółkę usunięte. Jednocześnie należy wskazać, iż Generalny Inspektor uwzględniając wyjaśnienia strony dotyczące podjęcia działań zmierzających do przywrócenia stanu zgodnego z prawem, wyznaczył miesięczny termin wykonania punktu 2 sentencji niniejszej decyzji.

Zgodnie z częścią A pkt IV ust. 3 załącznika do rozporządzenia, dane osobowe przetwarzane w systemie informatycznym zabezpiecza się przez wykonywanie kopii zapasowych zbiorów danych oraz programów służących do przetwarzania danych.

W toku czynności kontrolnych ustalono, że dane osobowe członków wspólnoty mieszkaniowej przetwarzane przez Spółkę przy użyciu systemu informatycznego o nazwie „XYZ” nie są zabezpieczone przez wykonywanie kopii zapasowych tworzonych na zewnętrznych nośnikach.

W odpowiedzi na zawiadomienie o wszczęciu postępowania administracyjnego Spółka pismem z dnia 22 sierpnia 2011 r. poinformowała Generalnego Inspektora o usunięciu ww. uchybienia, jednak nie potwierdziła tego oświadczenia żadnymi dokumentami takimi jak np. procedura wykonywania kopii zapasowych. Z uwagi na powyższe uznać należy, iż ww. uchybienie nie zostało usunięte.

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.