GENERALNY INSPEKTOR OCHRONY DANYCH OSOBOWYCH

dr Wojciech R. Wiewiórowski

Warszawa, dnia 27 kwietnia 2012 r.

DIS/DEC-384/12/27641

dot. [...]

D E C Y Z J A

Na podstawie 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 i art. 22 w związku z art. 31 ust. 3 i art. 38 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 pkt 1 i 3 oraz § 5 pkt 6 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) oraz częścią A pkt III ppkt 1 i pkt IV ust. 1 załącznika do ww. rozporządzenia, po przeprowadzeniu postępowania administracyjnego w sprawie przetwarzania danych osobowych przez Panią J. B. prowadzącą działalność gospodarczą pod nazwą „M",

umarzam postępowanie w niniejszej sprawie.

Uzasadnienie

Inspektorzy, upoważnieni przez Generalnego Inspektora Ochrony Danych Osobowych, przeprowadzili u Pani J. B. prowadzącej działalność gospodarczą pod nazwą „M"., zwanej dalej Przedsiębiorcą, kontrolę 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 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 również rozporządzeniem. W toku kontroli odebrano od Przedsiębiorcy i jego pracowników 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 Przedsiębiorcę.

W toku kontroli ustalono, że Przedsiębiorca przetwarza dane osobowe członków Wspólnoty Mieszkaniowej […], jako podmiot, któremu Wspólnota Mieszkaniowa […], jako administrator tych danych, powierzyła ich przetwarzanie zgodnie z art. 31 ust. 1 ustawy, na podstawie umowy o administrowanie nieruchomością zawartej w dniu […] sierpnia 2011 r.

Stosownie zaś 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.

Na podstawie materiału dowodowego zgromadzonego w niniejszej sprawie ustalono, że Przedsiębiorca naruszył przepisy o ochronie danych osobowych. Uchybienia polegały na:

1. Niezabezpieczeniu systemu informatycznego o nazwie „S”, służącego do przetwarzania danych osobowych, przed działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego (część A pkt III ppkt 1 załącznika do rozporządzenia).
2. Posługiwaniu się przez pracownika zatrudnionego na stanowisku księgowej identyfikatorami do systemu operacyjnego „W” i systemu informatycznego o nazwie „S”, które należały poprzednio do innego pracownika (część A pkt IV ust. 1 załącznika do rozporządzenia).
3. Nieuwzględnieniu w prowadzonej przez Przedsiębiorcę polityce bezpieczeństwa wykazu budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe, a ponadto, nieuwzględnieniu w opisie struktury zbiorów danych wskazującym zawartość poszczególnych pól informacyjnych i powiązania między nimi, dotyczącym systemu „S”, wszystkich pól informacyjnych, w tym następujących: typ lokalu, powierzchnia użytkowa, liczba

osób, identyfikator lokalu, powierzchnia obliczeniowa, dodatkowa, funkcyjna, stan lokalu, uwagi (§ 4 pkt 1 i 3 rozporządzenia).

4. Niewskazaniu w prowadzonej przez Przedsiębiorcę instrukcji zarządzania systemem informatycznym sposobu zabezpieczenia systemu informatycznego o nazwie „S" przed działalnością oprogramowania, o którym mowa w pkt III ppkt 1 załącznika do rozporządzenia (§ 5 pkt 6 rozporządzenia).

5. Niezapewnieniu, aby system informatyczny o nazwie „S" zapewniał sporządzenie i wydrukowanie raportu zawierającego w powszechnie zrozumiałej formie informacje o dacie pierwszego wprowadzenia danych osobowych do systemu (art. 38 ustawy).

W związku z powyższym, Generalny Inspektor Ochrony Danych Osobowych wszczął z urzędu postępowanie administracyjne w niniejszej sprawie w celu wyjaśnienia okoliczności sprawy. W piśmie z dnia […] marca 2012 r. zawiadamiającym o wszczęciu postępowania administracyjnego w przedmiotowej sprawie […], Przedsiębiorca został poinformowany 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, Przedsiębiorca w piśmie z dnia [...] marca 2012 r. złożył wyjaśnienia, w których poinformował m.in., że:

1. System informatyczny „S" nie posiada programu antywirusowego, jednak ze względu na bezpieczeństwo zawartych w nim danych posiada wdrożone następujące zabezpieczenia: serwer bazy danych jest fizycznie odseparowany od sieci zewnętrznej i wewnętrznej; autoryzacja użytkowników następuje poprzez hasła dostępu; system posiada indywidualną niezależną drukarkę; wszelkie dane są wprowadzane do tego systemu ręcznie. Powyższe zabezpieczenia uniemożliwiają przedostanie się do systemu informatycznego „S" programów szpiegowskich oraz wirusów komputerowych, w tym uszkodzenie, zafałszowanie lub przechwycenie danych.

2. Identyfikator pracownika zatrudnionego na stanowisku księgowej, należący do innego pracownika został zmieniony.

3. Polityka bezpieczeństwa została uzupełniona o wykaz pomieszczeń, w których są przetwarzane dane osobowe.

4. W opisie struktury zbiorów danych dotyczącym systemu informatycznego „S" uwzględniono pola informacyjne, których brak stwierdzono w toku kontroli.

5. Instrukcję zarządzania systemem informatycznym uzupełniono o sposób zabezpieczenia systemu informatycznego.

6. System informatyczny „S” zapewnia sporządzenie i wydrukowanie raportu zawierającego informacje o dacie pierwszego wprowadzenia danych osobowych do systemu.

W załączeniu do ww. pisma, jako dowody mające potwierdzić złożone wyjaśnienia, przesłano: „Instrukcję zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych w […], „Politykę bezpieczeństwa danych osobowych w […] wraz z załącznikiem nr 1 - „Opis zawartości zbiorów” oraz wydruk z systemu informatycznego o nazwie „S”. Ponadto, w dniu […] kwietnia 2012 r. przesłano kserokopię załącznika nr […] do „Polityki bezpieczeństwa danych osobowych w […] zawierającego „Wykaz pomieszczeń w których przetwarzane są dane osobowe”.

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

Na podstawie wyjaśnień złożonych przez Przedsiębiorcę w piśmie z dnia […] marca 2012 r., jak również pozostałych załączonych do pisma dowodów należy stwierdzić, że uchybienia w procesie przetwarzania danych osobowych stanowiące przedmiot postępowania zostały usunięte, tj.:

1. System informatyczny o nazwie „S”, służący do przetwarzania danych osobowych, został zabezpieczony przed działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego.
2. Zapewniono, aby identyfikator użytkownika, który utracił uprawnienia do przetwarzania danych, nie był przydzielony innej osobie.
3. W dokumencie o nazwie „Polityka bezpieczeństwa danych osobowych w […] wskazano wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe, a ponadto, w opisie struktury zbiorów danych wskazującym zawartość poszczególnych pól informacyjnych i powiązania między nimi, dotyczącym systemu „S”, uwzględniono wszystkie pola informacyjne, w tym: typ lokalu, powierzchnia użytkowa, liczba osób, identyfikator lokalu, powierzchnia obliczeniowa, dodatkowa, funkcyjna, stan lokalu, uwagi.
4. W dokumencie o nazwie „Instrukcja zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych w […] wskazano sposób zabezpieczenia systemu informatycznego o nazwie „S” przed działalnością oprogramowania, o którym mowa w pkt III ppkt 1 załącznika do rozporządzenia.
5. System informatyczny o nazwie „S” zapewnia sporządzenie i wydrukowanie raportu zawierającego w powszechnie zrozumiałej formie informacje o dacie pierwszego wprowadzenia danych osobowych do systemu.

Stosownie do art. 105 § 1 Kodeksu postępowania administracyjnego, gdy postępowanie z jakiejkolwiek przyczyny stało się bezprzedmiotowe w całości albo w części, organ administracji publicznej wydaje decyzję o umorzeniu postępowania odpowiednio w całości albo w części. Przesłanką umorzenia postępowania, na podstawie art. 105 § 1 k.p.a. jest bezprzedmiotowość postępowania „z jakiejkolwiek 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).

Na podstawie całokształtu materiału dowodowego zebranego w niniejszej sprawie uznać należy, iż w toku postępowania usunięte zostały uchybienia w procesie przetwarzania danych osobowych stanowiące przedmiot postępowania. Z powyższych względów postępowanie należało 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.