



**GENERALNY INSPEKTOR
OCHRONY DANYCH
OSOBOWYCH**

Michał Serzycki

Warszawa, dnia 15 stycznia 2010 r.

DIS/DEC-28/1778/10

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. 31 ust. 1, art. 36 ust. 2, art. 37, 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 ust. 1, § 7 ust. 1 pkt 1 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 IV ust. 1, częścią A pkt IV ust. 2, częścią B pkt VIII, częścią C pkt XIII załącznika do ww. rozporządzenia, po przeprowadzeniu postępowania administracyjnego w sprawie przetwarzania danych osobowych przez Panią A. B. prowadzącą działalność gospodarczą pod firmą „S”,

I. Nakazuję Pani A. B. prowadzącej działalność gospodarczą pod firmą „S”, usunięcie uchybień w procesie przetwarzania danych osobowych poprzez:

- 1. Zgłoszenie do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych zbioru danych osobowych użytkowników portalu internetowego o nazwie [...], w terminie od dnia, w którym niniejsza decyzja stanie się ostateczna.**
- 2. Zawarcie z S. s.c., umowy powierzenia przetwarzania danych osobowych, w terminie 30 dni od dnia, w którym niniejsza decyzja stanie się ostateczna.**
- 3. Opracowanie dokumentacji opisującej sposób przetwarzania danych osobowych oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych, tj. polityki bezpieczeństwa i instrukcji zarządzania systemem informatycznym służącym do**

przetwarzania danych osobowych, w terminie 30 dni od dnia, w którym niniejsza decyzja stanie się ostateczna.

4. Uzupełnienie ewidencji osób upoważnionych do przetwarzania danych osobowych poprzez wskazanie zakresu upoważnienia do przetwarzania danych oraz identyfikatora osoby upoważnionej, w terminie 7 dni od dnia, w którym niniejsza decyzja stanie się ostateczna.

5. Zapewnienie, aby hasła służące do uwierzytelniania pracowników w portalu internetowym o nazwie [...], składały się z co najmniej 8 znaków, zawierały małe i wielkie litery oraz cyfry lub znaki specjalne, w terminie 30 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

Inspektorzy upoważnieni przez Generalnego Inspektora Ochrony Danych Osobowych, przeprowadzili u Pani A. B. prowadzącej działalność gospodarczą pod firmą „S”, zwanej dalej również Przedsiębiorcą, kontrolę zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych sygn. kontroli [...], 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 ustne wyjaśnienia oraz skontrolowano system informatyczny służący do przetwarzania danych osobowych. Stan faktyczny został szczegółowo opisany w protokole kontroli i dołączonych do niego załącznikach. Protokół kontroli został podpisany przez Przedsiębiorcę.

Na podstawie tak zgromadzonego materiału dowodowego ustalono, że w procesie przetwarzania danych osobowych Pani A. B. prowadzącą działalność gospodarczą pod firmą „S”, jako administrator danych, naruszyła przepisy o ochronie danych osobowych. Uchybienia te polegały na:

1. Niezgłoszeniu do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych zbioru danych osób rejestrujących się na portalu internetowym [...] (art. 40 ustawy).
2. Niezawarciu z podmiotem, któremu Przedsiębiorca powierzył przetwarzanie danych osobowych umowy powierzenia przetwarzania danych (art. 31 ust. 1 ustawy).

3. Braku polityki bezpieczeństwa oraz instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych (art. 36 ust. 2 ustawy w związku z § 3 ust. 1 rozporządzenia).
4. Nienadaniu osobom przetwarzającym dane osobowe upoważnień do przetwarzania ww. danych (art. 37 ustawy).
5. Niezapewnieniu, aby portal internetowy o nazwie [...] umożliwiał odnotowanie daty pierwszego wprowadzenia danych do systemu (§ 7 ust. 1 pkt 1 rozporządzenia).
6. Braku ewidencji osób upoważnionych do przetwarzania danych osobowych (art. 39 ustawy).
7. Niezastosowaniu środków kryptograficznej ochrony wobec danych wykorzystywanych do uwierzytelnienia, które są przesyłane w sieci publicznej (część C pkt XIII załącznika do rozporządzenia).
8. Niezapewnieniu, aby identyfikator użytkownika, który utracił uprawnienia do przetwarzania danych, nie mógł być przydzielony innej osobie (część A pkt IV ust. 1 załącznika do rozporządzenia).
9. Niezapewnieniu, aby zmiana hasła wykorzystywanego podczas logowania się pracowników do portalu [...] następowała nie rzadziej, niż co 30 dni (część A pkt IV ust. 2 załącznika do rozporządzenia).
10. Niezapewnieniu, aby hasło używane do uwierzytelniania pracowników na portalu [...] składało się co najmniej z 8 znaków, zawierało małe i wielkie litery oraz cyfry lub znaki specjalne (część B pkt VIII załącznika do rozporządzenia).

W związku z powyższym, w dniu [...] października 2009 r. Generalny Inspektor Ochrony Danych Osobowych wszczął z urzędu postępowanie administracyjne w niniejszej sprawie w celu wyjaśnienia okoliczności sprawy sygn. pisma [...].

W odpowiedzi na zawiadomienie o wszczęciu postępowania administracyjnego Przedsiębiorca w piśmie z dnia [...] grudnia 2009 r. złożył wyjaśnienia, w których poinformował między innymi, że:

1. Niezwłocznie zgłosi do rejestracji zbiór danych osobowych użytkowników portalu internetowego o nazwie [...].
2. Dane osobowe użytkowników portalu internetowego o nazwie [...] umieszczone są na serwerze wynajmowanym od S. s.c. Wskazany podmiot zabezpiecza serwer i umieszczone na nim dane.
3. Dokumentacja opisująca sposób przetwarzania danych osobowych oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych, tj. polityka bezpieczeństwa i instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych jest w trakcie opracowywania.

4. Osobom dopuszczonym do przetwarzania danych osobowych nadano stosowne upoważnienia.

5. Opracowano ewidencję osób upoważnionych do przetwarzania danych osobowych.

6. Portal internetowy o nazwie [...] zapewnia odnotowania daty pierwszego wprowadzenia danych do systemu.

7. Wdrażana jest kryptograficzna ochrona danych przesyłanych w związku z funkcjonowaniem portalu [...].

8. Portal internetowy [...] zmodyfikowano w ten sposób, iż użytkownik nie ma możliwości posługiwania się identyfikatorem osoby, która utraciła uprawnienia do przetwarzania danych.

9. Hasła wykorzystywane podczas logowania się do portalu [...] zmieniane są co 30 dni, a minimalna długość ww. haseł wynosi 8 znaków.

Do pisma z dnia [...] grudnia 2009 r., jako dowody mające potwierdzić przesłane wyjaśnienia, załączono: wydruk zrzutu ekranu z uwidocznioną funkcjonalnością kryptograficznej ochrony przesyłanych danych, wydruk zrzutu ekranu z uwidocznioną datą wprowadzenia danych do systemu, wydruk zrzutu ekranu z informacją dotyczącą parametrów hasła, wydruk zrzutu ekranu z informacjami dotyczącymi identyfikatora użytkownika, kserokopię ewidencji osób upoważnionych do przetwarzania danych osobowych, kserokopie upoważnień do przetwarzania danych osobowych.

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

Zgodnie z art. 40 ustawy, administrator danych jest obowiązany zgłosić zbiór danych do rejestracji Generalnemu Inspektorowi, z wyjątkiem przypadków, o których mowa w art. 43 ust. 1 ustawy. Natomiast zgodnie z art. 7 pkt 1 ustawy, ilekroć w ustawie jest mowa o zbiorze danych rozumie się przez to każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie. W myśl art. 6 ust. 1 ustawy, za dane osobowe uważa się wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. Osobą możliwą do zidentyfikowania jest osoba, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności przez powołanie się na numer identyfikacyjny albo jeden lub kilka specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne.

W toku kontroli ustalono, że aby założyć konto na portalu [...] zainteresowana osoba musi wypełnić formularz zamieszczony na stronie internetowej i podać dane takie jak: nick, e-mail oraz hasło. Po założeniu konta użytkownik ma możliwość uzupełnienia swojego profilu o elementy

wymagane (imię, województwo, choroba i jej objawy) oraz inne dane (w tym informacje o nałogach), których podanie oznaczone jest jako dobrowolne. Należy uznać, iż pozyskiwane od użytkowników ww. portalu dane, zwłaszcza adresy e-mail składające się z imienia i nazwiska oraz choroby i ich opisy (mogące być bardzo rzadkie, występujące na terenie kraju w jednym lub kilku przypadkach) stanowią informacje dotyczące osoby możliwej do zidentyfikowania, a tym samym spełniają kryteria definicji danych osobowych, sformułowanej w powołanym art. 6 ustawy. Z tego względu przetwarzanie ww. informacji przez Przedsiębiorcę podlega rygorom ustawy o ochronie danych osobowych.

W związku z tym, iż dane użytkowników portalu internetowego [...], stanowią zbiór w rozumieniu art. 7 pkt 1 ustawy i nie zachodzą przesłanki wskazane w art. 43 ust. 1 ustawy, ww. zbiór danych powinien zostać zgłoszony do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych. Mając na uwadze, że ww. zbiór nie został zgłoszony do rejestracji, pomimo złożenia przez Przedsiębiorcę w piśmie z dnia [...] grudnia 2009 r. deklaracji dokonania wskazanego zgłoszenia, należy uznać, iż w ww. zakresie uchybienie w procesie przetwarzania danych osobowych nie zostało usunięte.

Zgodnie z art. 31 ust. 1 ustawy, administrator danych może powierzyć innemu podmiotowi, w drodze umowy zawartej na piśmie, przetwarzanie danych.

W toku kontroli ustalono, że portal internetowy o nazwie [...] umieszczony jest na serwerze dzierżawionym od S. s.c. Zgodnie z wyjaśnieniami Przedsiębiorcy zawartymi w piśmie z dnia [...] grudnia 2009 r. ww. podmiot zabezpiecza serwer i umieszczone na nim dane. Jako umowę, na podstawie której powierzono przetwarzanie danych osobowych związanych z funkcjonowaniem portalu internetowego [...]. Przedsiębiorca wskazał umowę z dnia [...] grudnia 2008 r. Wskazana umowa nie zawiera zakresu i celu przetwarzania danych osobowych, co stanowi *essentialia negoti* umowy powierzenia przetwarzania danych osobowych. Ponadto, żadne z postanowień powołanej umowy nie wskazuje na to, iż dzierżawa ww. serwera odbywa się w związku z przetwarzaniem danych osobowych na portalu [...]. Wobec powyższego brak jest podstaw do uznania wskazanej umowy jako umowy powierzenia przetwarzania danych osobowych, o której mowa w art. 31 ust. 1 ustawy.

Zgodnie z art. 36 ust. 2 ustawy, administrator danych prowadzi dokumentację opisującą sposób przetwarzania danych oraz środki, o których mowa w ust. 1. Natomiast 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”.

W toku czynności kontrolnych ustalono, że Przedsiębiorca nie posiada dokumentacji opisującej sposób przetwarzania danych oraz środki, o których mowa w art. 36 ust. 1 ustawy,

tj. polityki bezpieczeństwa i instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych. Należy wskazać, iż zawarta w wyjaśnieniach Przedsiębiorcy z dnia [...] grudnia 2009 r. informacja o rozpoczęciu prac nad ww. dokumentacją nie może być podstawą uznania, iż związane z tym uchybienie w procesie przetwarzania danych osobowych zostało usunięte.

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.

Analiza nadesłanej przez Przedsiębiorcę ewidencji osób upoważnionych do przetwarzania danych osobowych wykazała, iż powołany dokument nie zawiera informacji dotyczących zakresu upoważnienia do przetwarzania danych osobowych oraz identyfikatora osoby upoważnionej do przetwarzania danych.

Zgodnie z częścią B pkt VIII załącznika do rozporządzenia, w przypadku, gdy do uwierzytelniania użytkowników używa się hasła, składa się ono, co najmniej z 8 znaków, zawiera małe i wielkie litery oraz cyfry lub znaki specjalne.

W toku czynności kontrolnych ustalono, że portal [...] obsługiwany jest przez Internet, a wymagana minimalna długość hasła użytkownika ww. portalu wynosi sześć znaków. W wyjaśnieniach zawartych w piśmie z dnia [...] września 2009 r. Przedsiębiorca wskazał, iż hasło wykorzystywane podczas logowania się pracowników do ww. portalu składa się z około 10 znaków i są to cyfry oraz litery wykorzystywane na przemian. Ponadto, w piśmie z dnia [...] grudnia 2009 r. Przedsiębiorca wyjaśnił, iż minimalna długość ww. hasła wynosi 8 znaków, na dowód czego przesłany został wydruk zrzutu ekranu zawierający informację o minimalnej długości hasła. Na podstawie przedstawionych przez Przedsiębiorcę dowodów należy uznać, iż zapewniono aby długość hasła spełniała wymogi wskazane w rozporządzeniu. Natomiast ww. dowody nie potwierdzają wymaganej przepisami rozporządzenia złożoności hasła w zakresie małych i wielkich liter oraz cyfr lub znaków specjalnych. Należy wskazać, iż hasło wykorzystywane do uwierzytelniania użytkowników w systemie informatycznym powinno zawierać łącznie wszystkie elementy wskazane w cytowanym przepisie rozporządzenia. Brak któregośkolwiek z wymienionych elementów powoduje, iż zastosowane hasło nie spełniałoby wyznaczonej mu funkcji. W związku z powyższym, uchybienie w tym zakresie należy uznać za nieusunięte.

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

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

2. Opracowano ewidencję osób upoważnionych do przetwarzania danych osobowych, która zawiera między innymi imię i nazwisko upoważnionej osoby oraz datę nadania i ustania upoważnienia do przetwarzania danych osobowych.
3. Zapewniono, aby portal internetowy [...] umożliwiał odnotowanie daty pierwszego wprowadzenia danych do systemu.
4. Zastosowano środki kryptograficznej ochrony wobec danych wykorzystywanych do uwierzytelnienia, które są przesyłane w sieci publicznej.
5. Zapewniono, aby identyfikator użytkownika, który utracił uprawnienia do przetwarzania danych, nie mógł być przydzielony innej osobie.
6. Zapewniono, aby zmiana haseł służących do uwierzytelniania pracowników w portalu [...] następowała 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.