



**GENERALNY INSPEKTOR
OCHRONY DANYCH
OSOBOWYCH**

dr Wojciech R. Wiewiórowski

Warszawa, dnia 10 czerwca 2011 r.

DIS/DEC-476/27863/11

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.) oraz art. 12 pkt 2 i art. 22 w związku z art. 36 ust. 1 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.) oraz częścią A pkt IV ust. 2, częścią B pkt VIII i częścią C pkt XIII załącznika do 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 Pana A. K. prowadzącego działalność gospodarczą pod firmą P.,

u m a r z a m p o s t ę p o w a n i e w n i n i e j s z e j s p r a w i e.

Uzasadnienie

Inspektorzy upoważnieni przez Generalnego Inspektora Ochrony Danych Osobowych przeprowadzili kontrolę sygn. akt [...] u Pana A. K. prowadzącego działalność gospodarczą pod firmą P. (zwanym dalej Przedsiębiorcą) 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. z 2004 r. Nr 100, poz. 1024), zwanym dalej rozporządzeniem. W toku kontroli odebrano od pełnomocnika Przedsiębiorcy ustne wyjaśnienia, skontrolowano systemy informatyczne służące do przetwarzania danych osobowych oraz dokonano oględzin pomieszczeń, w których odbywa się przetwarzanie danych osobowych. Ustalony stan faktyczny został szczegółowo opisany w protokole kontroli, który został podpisany przez pełnomocnika Przedsiębiorcy.

Na podstawie całokształtu materiału dowodowego zgromadzonego w sprawie ustalono, że w procesie przetwarzania danych osobowych Przedsiębiorca, jako administrator danych osobowych naruszył przepisy o ochronie danych osobowych. Stwierdzone uchybienia polegały na:

1. Niezastosowaniu wobec danych osobowych kandydatów do pracy pozyskanych za pomocą formularza rejestracyjnego, zamieszczonego na stronie internetowej o adresie: [...] odpowiednich środków technicznych i organizacyjnych, w celu ochrony tych danych przed ich udostępnieniem osobom nieupoważnionym, gdyż ich przesyłanie do bazy danych umieszczonej na serwerze będącym własnością firmy I. Sp. z o.o. odbywa się łączami nieszyfrowanymi (art. 36 ust. 1 ustawy).

2. Niezastosowaniu wobec danych osobowych kandydatów do pracy otrzymanych w e-mailach odpowiednich środków technicznych i organizacyjnych, w celu ochrony tych danych przed ich udostępnieniem osobom nieupoważnionym, gdyż ich przesyłanie do agencji partnerskich odbywa się łączami nieszyfrowanymi (art. 36 ust. 1 ustawy).

3. Niezastosowaniu zgodnie z częścią C pkt XIII załącznika do rozporządzenia, środków kryptograficznej ochrony wobec danych wykorzystywanych do:

- uwierzytelniania do bazy danych kandydatów do pracy zamieszczonej na serwerze będącym własnością firmy I. Sp. z o.o., które są przesyłane w sieci publicznej;

- uwierzytelniania zarejestrowanych użytkowników na stronie internetowej o adresie [...].

4. Niezapewnieniu, możliwości zmiany haseł nie rzadziej niż co 30 dni: dla użytkowników strony internetowej o adresie [...] oraz dla użytkowników systemu operacyjnego Windows XP (służącego do odbierania e-maili od kandydatów do pracy oraz wysyłania e-maili do agencji partnerskich) - część A pkt IV ust. 2 załącznika do rozporządzenia.

5. Niezapewnieniu, aby hasło używane do uwierzytelnienia użytkownika strony internetowej o adresie [...] 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, 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 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 pismem z dnia [...] kwietnia 2011 r. pełnomocnik Przedsiębiorcy przesłał wyjaśnienia w zakresie stwierdzonych uchybień, z których wynika, że:

1. Wdrożony został certyfikat SSL zapewniający szyfrowanie przesyłanych danych osobowych kandydatów do pracy pozyskanych za pomocą formularza rejestracyjnego, zamieszczonego na stronie internetowej o adresie: [...], a przesyłanych do bazy danych umieszczonej na serwerze będącym własnością firmy I. Sp. z o.o. Wprowadzono procedurę przesyłania danych osobowych kandydatów do pracy do agencji partnerskich w sposób zaszyfrowany. Przesyłane dane osobowe zawarte są w załączonych plikach dokumentu w formacie Word, które zabezpieczone są indywidualnym hasłem. Osoba upoważniona do odbioru dokumentu otwiera dokument z zawartymi danymi po wpisaniu wymaganego hasła.

3. Zastosowano kryptograficzne środki ochrony danych wobec danych wykorzystywanych do uwierzytelniania do bazy danych kandydatów do pracy zamieszczonej na serwerze będącym własnością firmy I. Sp. z o.o., które są przesyłane w sieci publicznej.

4. Zastosowano kryptograficzne środki ochrony danych wobec danych wykorzystywanych do uwierzytelniania zarejestrowanych użytkowników na stronie internetowej o adresie [...].

5. Wprowadzono funkcjonalność wymuszającą zmianę haseł co 30 dni dla użytkowników strony internetowej o adresie [...] oraz haseł do systemu operacyjnego Windows XP komputerów służących do odbierania m. in. e-maili od kandydatów do pracy oraz wysyłania e-maili do agencji partnerskich.

6. Hasło używane do uwierzytelnienia użytkownika strony internetowej o adresie [...] składała się co najmniej z 8 znaków, zawiera małe i wielkie litery oraz cyfry.

Ponadto, do ww. pisma załączono dokumenty potwierdzające złożone wyjaśnienia w postaci: dwóch przykładowych wydruków ze strony internetowej o adresie [...]; wydruku przykładowego dokumentu w formacie Word; wydruk dokumentu o nazwie „Regulaminu/polityki prywatności” oraz kserokopii dokumentu o nazwie „Procedury – rozpoczęcie /zawieszenie/zakończenie pracy”.

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

W świetle złożonych przez pełnomocnika Przedsiębiorcy wyjaśnień oraz załączonych dokumentów należy uznać, że stwierdzone w toku kontroli uchybienia w procesie

przetwarzania danych osobowych, stanowiące przedmiot niniejszego postępowania, zostały usunięte.

Stosownie do art. 105 § 1 Kodeksu postępowania administracyjnego, gdy postępowanie z jakiegokolwiek 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 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/Sz 1029/97). W toku niniejszego postępowania usunięte zostały uchybienia w procesie przetwarzania danych osobowych, stanowiące przedmiot niniejszego 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.