



**GENERALNY INSPEKTOR
OCHRONY DANYCH
OSOBOWYCH**

Michał Serzycki

Warszawa, dnia 24 sierpnia 2009 r.

DIS/DEC- 829/30716/09

dot. DIS-K-421/55/09

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. 36 ust. 2, art. 39 i 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.), § 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 urzędy i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100, poz. 1024), a także częścią A pkt II ust. 2 ppkt a i ppkt b, pkt IV ust. 2 i ust. 3 oraz częścią B pkt VIII załącznika do powołanego rozporządzenia, po przeprowadzeniu postępowania administracyjnego w sprawie przetwarzania danych osobowych przez XY Sp. z o.o. z siedzibą w (...),

I. Nakazuję XY Sp. z o.o. z siedzibą w (...), usunięcie uchybień w procesie przetwarzania danych osobowych, poprzez uzupełnienie polityki bezpieczeństwa o opis struktury zbiorów danych wskazującego 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 1 miesiąca od dnia, w którym niniejsza decyzja stanie się ostateczna.

II. W pozostałym zakresie postępowanie umarzam.

Uzasadnienie

Inspektorzy, upoważnieni przez Generalnego Inspektora Ochrony Danych Osobowych przeprowadzili kontrolę w XY Sp. z o.o. z siedzibą w (...), zwaną dalej także Spółką w celu ustalenia zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych (sygn. DIS-K-....), 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 materiału dowodowego zgromadzonego w toku kontroli ustalono, że w procesie przetwarzania danych XY Sp. z o.o. z siedzibą w...., jako administrator danych, naruszyła przepisy o ochronie danych osobowych. Uchybienia te polegały na:

1. Niezapewnieniu, aby w systemie informatycznym o nazwie „FAST” (w którym przetwarzane są dane osobowe klientów Spółki) rejestrowany był dla każdego użytkownika odrębny identyfikator (część A pkt II ust. 2 ppkt a załącznika do rozporządzenia).
2. Niezapewnieniu, aby dostęp do danych w systemie informatycznym o nazwie „FAST” był możliwy wyłącznie po wprowadzeniu identyfikatora i dokonaniu uwierzytelnienia (część A pkt II ust. 2 ppkt b załącznika do rozporządzenia).
3. Niezapewnieniu, aby hasło używane do uwierzytelnienia użytkownika w systemie o nazwie „FAST” był zmieniane nie rzadziej, niż co 30 dni (część A pkt IV ust. 2 załącznika do rozporządzenia).
4. Niezapewnieniu, aby dane osobowe przetwarzane w systemie informatycznym o nazwie „FAST” były zabezpieczone przez wykonanie kopii zapasowych zbiorów danych oraz programów służących do przetwarzania danych (część A pkt IV ust. 3 załącznika do rozporządzenia).
5. Niezapewnieniu, aby do uwierzytelniania użytkowników w systemie informatycznym o nazwie „FAST” hasło składało się, co najmniej z 8 znaków, zawierało małe i wielkie litery oraz cyfry lub znaki specjalne (część B pkt VIII załącznika do rozporządzenia).

6. Nieuzupełnieniu ewidencji osób upoważnionych do przetwarzania danych osobowych (art. 39 ustawy).
7. Niezgłoszeniu do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych zbioru danych klientów Spółki - osób korzystających z toru do jazdy samochodem wyścigowym, kartingiem (art. 40 ustawy).
8. Nieuzupełnieniu 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 wskazującego 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 (§ 4 rozporządzenia).

W piśmie z dnia 27 maja 2009 r. (sygn. DIS-K-421/55/09/19258), stanowiącym zawiadomienie o wszczęciu postępowania administracyjnego w przedmiotowej sprawie, XY Sp. z o.o. z siedzibą w (...) 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.

W odpowiedzi na zawiadomienie o wszczęciu postępowania administracyjnego Członek Zarządu Spółki, pismem z dnia 02 lipca 2009 r. złożył wyjaśnienia, w których poinformował, iż:

- 1) w systemie informatycznym o nazwie „FAST” (w którym przetwarzane są dane osobowe klientów Spółki) rejestrowany jest dla każdego użytkownika odrębny identyfikator,
- 2) dostęp do danych w systemie informatycznym o nazwie „FAST” jest możliwy wyłącznie po wprowadzeniu identyfikatora i dokonaniu uwierzytelnienia,
- 3) zmiana hasła używanego do uwierzytelnienia użytkownika w systemie o nazwie „FAST” następuje nie rzadziej, niż co 30 dni,
- 4) dane osobowe przetwarzane w systemie informatycznym o nazwie „FAST” są zabezpieczone przez wykonanie kopii zapasowych zbiorów danych oraz programów służących do przetwarzania danych,
- 5) do uwierzytelniania użytkowników w systemie informatycznym o nazwie „FAST” hasło składa się, co najmniej z 8 znaków, zawiera małe i wielkie litery oraz cyfry lub znaki specjalne,
- 6) zgłoszono do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych zbiór danych o nazwie „XY Sp. z o.o.”.

Do wskazanych wyjaśnień załączono następujące dokumenty: wydruk polityki bezpieczeństwa, wydruk polityki prywatności, wydruk listy budynków i pomieszczeń gdzie dane są przetwarzane, wydruk topologii połączeń między komputerami, wydruk listy modułów oprogramowania o nazwie „FAST” z poziomu użytkowników i zbiorami danych ze wskazaniem na programy użyte do przetwarzania danych, wydruk instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w XY wraz z wydrukiem zarządzenia administratora danych osobowych Nr 1/2009 w sprawie zmian zasad logowania użytkowników do systemu FAST w związku z jego aktualizacją, wydruk zarządzenia Nr 1/2006 z dnia 1 października 2006 r. w sprawie wprowadzenia w XY „Regulaminu w zakresie przetwarzania danych osobowych w XY” wraz z wydrukiem powołanego Regulaminu, wydruk ewidencji osób upoważnionych do przetwarzania danych osobowych w systemie XY, wydruk zgłoszonego do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych zbioru danych o nazwie „XY Sp. z o.o.”.

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

Zgodnie z art. 36 ust. 2 ustawy, administrator danych prowadzi dokumentację opisującą sposób przetwarzania danych oraz środki, o których mowa w ust. 1. 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. Zgodnie z ust. 2, dokumentację, o której mowa w § 1 pkt 1, prowadzi się w formie pisemnej.

Natomiast zgodnie z § 4 pkt 3, pkt 4 i pkt 5 rozporządzenia, polityka bezpieczeństwa, o której mowa w § 3 ust. 1, zawiera w szczególności: opis struktury zbiorów danych wskazującego 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 toku czynności kontrolnych ustalono, że w Spółce jest prowadzona dokumentacja opisująca sposób przetwarzania danych oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, tj. polityka bezpieczeństwa oraz instrukcja zarządzania systemem informatycznym.

W polityce bezpieczeństwa nie uwzględniono jednak wymogów określonych § 4 rozporządzenia, tj. ww. dokument nie zawiera: opisu struktury zbiorów danych wskazującego zawartość poszczególnych pól informacyjnych i powiązania między nimi (§ 4 pkt 3

rozporządzenia); sposobu przepływu danych pomiędzy poszczególnymi systemami (§ 4 pkt 4 rozporządzenia); określenia środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych (§ 4 pkt 5 rozporządzenia).

Jednocześnie, na podstawie złożonych wyjaśnień oraz przedstawionych dowodów, należy stwierdzić, że pozostałe uchybienia w procesie przetwarzania danych osobowych, stanowiące przedmiot postępowania, zostały usunięte, tj.:

- 1) zapewniono, aby w systemie informatycznym o nazwie „FAST” rejestrowany był dla każdego użytkownika odrębny identyfikator,
- 2) zapewniono, aby dostęp do danych w systemie informatycznym o nazwie „FAST” był możliwy wyłącznie po wprowadzeniu identyfikatora i dokonaniu uwierzytelnienia,
- 3) zapewniono, aby hasło używane do uwierzytelnienia użytkownika w systemie o nazwie „FAST” było zmieniane nie rzadziej, niż co 30 dni,
- 4) zapewniono, aby dane osobowe przetwarzane w systemie informatycznym o nazwie „FAST” były zabezpieczone przez wykonanie kopii zapasowych zbiorów danych oraz programów służących do przetwarzania danych,
- 5) zapewniono, aby do uwierzytelniania użytkowników w systemie informatycznym o nazwie „FAST” hasło składało się, co najmniej z 8 znaków, zawierało małe i wielkie litery oraz cyfry lub znaki specjalne,
- 6) uzupełniono ewidencję osób upoważnionych do przetwarzania danych osobowych,
- 7) zgłoszono do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych zbiór danych o nazwie „XY Sp. z o.o.” (zgłoszenie nr R: 003849/09).

Ponadto Członek Zarządu Spółki do pisma z dnia 02 lipca 2009 r. załączył m.in. wydruk listy budynków i pomieszczeń gdzie dane są przetwarzane oraz wydruk listy modułów oprogramowania o nazwie „FAST” z poziomu użytkowników i zbiorami danych ze wskazaniem na programy użyte do przetwarzania danych. Wobec powyższego uznać należy, iż polityka bezpieczeństwa spełnia wymogi, o których mowa § 4 pkt 1 i pkt 2 rozporządzenia. Należy jednak podnieść, iż powołane wyżej dokumenty zgodnie z § 4 rozporządzenia, winny być zawarte w polityce bezpieczeństwa. Reasumując, zasadne byłoby aby powołane wyżej dokumenty zostały załączone bądź też powołane w polityce bezpieczeństwa.

Stosownie do art. 105 § 1 Kodeksu postępowania administracyjnego, gdy postępowanie z jakiegokolwiek przyczyny stało się bezprzedmiotowe, organ administracji publicznej wydaje decyzję o jego umorzeniu. Jak stwierdził Naczelny Sąd Administracyjny w uzasadnieniu wyroku z dnia 19 listopada 2001 r. (sygn. akt II SA 2702/00): „(...) skoro w toku prowadzonego (...)

postępowania administracyjnego zniesiony został stan naruszenia prawa, którego miało dotyczyć rozstrzygnięcie, to postępowanie stało się bezprzedmiotowe”.

W związku z tym, że w toku postępowania usunięte zostały pozostałe uchybienia w procesie przetwarzania danych osobowych, stanowiące przedmiot postępowania, w tym zakresie należało je umorzyć.

Mając powyższe na uwadze, w tym stanie prawnym i faktycznym, 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.

