



**GENERALNY INSPEKTOR
OCHRONY DANYCH
OSOBOWYCH**

Michał Serzycki

Warszawa, dnia 12 października 2009 r.

DIS/DEC- 999/37016/09

dot. DIS-K-421/134/09

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. 26 ust. 1 pkt 1 i art. 39 ust. 1 pkt 3 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r., Nr 101, poz. 926 z późn. zm.), § 5 i § 7 ust. 1 pkt 1 i pkt 2 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 II ust. 1 i ust. 2 oraz częścią A pkt III ppkt 1 załącznika do rozporządzenia, po przeprowadzeniu postępowania administracyjnego w sprawie przetwarzania danych osobowych przez Specjalistyczną Spółdzielnię Pracy „XYZ” z siedzibą w (...),

- I. Nakazuję Specjalistycznej Spółdzielni Pracy „XYZ” z siedzibą w (...) usunięcie uchybień w procesie przetwarzania danych osobowych poprzez:**
- 1. Uzupełnienie ewidencji osób upoważnionych do przetwarzania danych osobowych o identyfikator użytkownika w systemie informatycznym, w terminie 7 dni od dnia, w którym niniejsza decyzja stanie się ostateczna.**
 - 2. Opracowanie instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, w terminie 30 dni od dnia, w którym niniejsza decyzja stanie się ostateczna.**

3. **Zmodyfikowanie systemu informatycznego o nazwie „Ramzes” w taki sposób, aby zapewniał dla każdej osoby, której dane osobowe są przetwarzane w systemie informatycznym, odnotowanie daty pierwszego wprowadzenia danych do systemu i identyfikatora użytkownika wprowadzającego dane osobowe do systemu, w terminie 6 miesięcy od dnia, w którym niniejsza decyzja stanie się ostateczna.**
4. **Zabezpieczenie systemu informatycznego o nazwie „Ramzes” przed działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego, w terminie 7 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 n i e

Inspektorzy upoważnieni przez Generalnego Inspektora Ochrony Danych Osobowych przeprowadzili kontrolę w Specjalistycznej Spółdzielni Pracy „XYZ” z siedzibą w (...), zwaną dalej Spółdzielnią, w celu ustalenia zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych (sygn. akt 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 Spółdzielni ustne wyjaśnienia, skontrolowano system informatyczny oraz dokonano oględzin pomieszczeń, w których odbywa się przetwarzanie danych osobowych. Stan faktyczny został szczegółowo opisany w protokole kontroli, który został podpisany przez Prezesa Zarządu Spółdzielni oraz członka Zarządu Spółdzielni.

Na podstawie tak zgromadzonego materiału dowodowego ustalono, że w procesie przetwarzania danych osobowych Spółdzielnia, jako administrator danych, naruszyła przepisy o ochronie danych osobowych. Uchybienia te polegały na:

1. Zbieraniu danych osobowych pracowników Spółdzielni w szerszym zakresie (o nazwisko rodowe matki) niż to wynika z przepisów ustawy z dnia 26 czerwca 1974 r. Kodeks pracy (Dz. U. z 1998 r., Nr 21, poz. 94 z późn. zm.).
2. Niezawarciu w ewidencji osób upoważnionych do przetwarzania danych osobowych identyfikatora użytkownika w systemie informatycznym.

3. Niezawarcia w obowiązującej w Spółdzielni „Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych” żadnego z elementów wymienionych w § 5 rozporządzenia.
4. Niezapewnianiu przez system informatyczny o nazwie „Ramzes” dla każdej osoby, której dane osobowe są przetwarzane w systemie informatycznym, odnotowania daty pierwszego wprowadzenia danych do systemu i identyfikatora użytkownika wprowadzającego dane osobowe do systemu.
5. Niezastosowaniu w systemie informatycznym o nazwie „Ramzes” mechanizmów kontroli dostępu do danych osobowych oraz umożliwieniu dostępu do danych przetwarzanych przy użyciu ww. systemu bez wprowadzenia identyfikatora i dokonania uwierzytelnienia.
6. Niezabezpieczeniu systemu informatycznego o nazwie „Ramzes” przed działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego.

W związku z powyższym, w dniu 10 września 2009 r. Generalny Inspektor Ochrony Danych Osobowych wszczął z urzędu postępowanie administracyjne w niniejszej sprawie w celu wyjaśnienia okoliczności sprawy (sygn. pisma DIS-K-....).

W odpowiedzi na zawiadomienie o wszczęciu postępowania administracyjnego Prezes Zarządu Spółdzielni oraz członek zarządu Spółdzielni pismem z dnia 22 września 2009 r., L.dz. 191/2009, złożyli wyjaśnienia, w których poinformowano, że:

1. Utworzone zostały dla dwóch osób odrębne identyfikatory wraz z hasłami dostępu do systemu Windows i programu płac.
2. Z dniem 21 września 2009 r. wprowadzony został do stosowania w Spółdzielni nowy druk kwestionariusza osobowego, który nie zawiera już nazwiska rodowego matki.
3. Z uwagi na bardzo trudną sytuację finansową Spółdzielnia nie jest w stanie w chwili obecnej wprowadzić bardziej nowoczesnego systemu informatycznego do obsługi płac.

Ponadto, do pisma z dnia 22 września 2009 r., L.dz. 191/2009, Prezes Zarządu Spółdzielni oraz członek zarządu Spółdzielni przedstawili dowody mające potwierdzić usunięcie uchybień stwierdzonych w toku kontroli.

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

Zgodnie z art. 39 ust. 1 pkt 3 ustawy, administrator danych prowadzi ewidencję osób upoważnionych do ich przetwarzania, która powinna zawierać identyfikator, jeżeli dane są przetwarzane w systemie informatycznym.

Przeprowadzona kontrola wykazała, że ewidencja osób upoważnionych do przetwarzania danych osobowych prowadzona jest w ramach dokumentu o nazwie „Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych”. Ewidencja ta nie zawiera jednak identyfikatora użytkownika w systemie informatycznym, co stanowi naruszenie powołanego przepisu ustawy. Należy także wskazać, że ze złożonych w odpowiedzi na zawiadomienie o wszczęciu postępowania administracyjnego wyjaśnień oraz załączonych dowodów nie wynika, aby Spółdzielnia podjęła działania mające na celu przywrócenie w tym zakresie stanu zgodnego z prawem.

Zgodnie z § 5 rozporządzenia, instrukcja, o której mowa w § 3 ust. 1, zawiera w szczególności: 1) procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym oraz wskazanie osoby odpowiedzialnej za te czynności; 2) stosowane metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem; 3) procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu; 4) procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania; 5) sposób, miejsce i okres przechowywania: a) elektronicznych nośników informacji zawierających dane osobowe, b) kopii zapasowych, o których mowa w pkt 4, 6) sposób zabezpieczenia systemu informatycznego przed działalnością oprogramowania, o którym mowa w pkt III ppkt 1 załącznika do rozporządzenia; 7) sposób realizacji wymogów, o których mowa w § 7 ust. 1 pkt 4; 8) procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych.

W toku kontroli ustalono, że obowiązująca w Spółdzielni „Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych” nie zawiera żadnego z elementów wymienionych w powołanym przepisie rozporządzenia, co stanowi jego naruszenie. Wskazać jednocześnie należy, że ze złożonych w odpowiedzi na zawiadomienie o wszczęciu postępowania administracyjnego wyjaśnień oraz załączonych dowodów nie wynika, aby Spółdzielnia podjęła działania mające na celu przywrócenie w tym zakresie stanu zgodnego z prawem.

Zgodnie z § 7 ust. 1 pkt 1 i pkt 2 rozporządzenia, dla każdej osoby, której dane osobowe są przetwarzane w systemie informatycznym - z wyjątkiem systemów służących do przetwarzania danych osobowych ograniczonych wyłącznie do edycji tekstu w celu udostępnienia go na piśmie - system ten zapewnia odnotowanie daty pierwszego wprowadzenia danych do systemu i identyfikatora użytkownika wprowadzającego dane osobowe do systemu, chyba że dostęp do systemu informatycznego i przetwarzanych w nim danych posiada wyłącznie jedna osoba.

Kontrola wykazała, że system informatyczny o nazwie „Ramzes” nie zapewnia dla każdej osoby, której dane osobowe są przetwarzane w systemie informatycznym, odnotowania daty pierwszego wprowadzenia danych do systemu i identyfikatora użytkownika wprowadzającego dane osobowe do systemu, co stanowi naruszenie ww. przepisu rozporządzenia.

W odpowiedzi na zawiadomienie o wszczęciu postępowania administracyjnego Prezes Zarządu Spółdzielni oraz członek zarządu Spółdzielni wyjaśnili, że z uwagi na bardzo trudną sytuację finansową Spółdzielnia nie jest w stanie w chwili obecnej wprowadzić bardziej nowoczesnego systemu informatycznego do obsługi płac. W związku z tym należy wskazać, że trudności finansowe administratora danych nie mogą być podstawą do zwolnienia go z obowiązku przetwarzania danych w sposób zgodny z przepisami o ochronie danych osobowych. Mogą natomiast stanowić okoliczność wpływającą na określenie terminu do przywrócenia stanu zgodnego z prawem. W niniejszej sprawie okoliczność ta została uwzględniona poprzez wyznaczenie 6-miesięcznego terminu na dostosowanie systemu informatycznego o nazwie „Ramzes” do wymogów wynikających z § 7 ust. 1 pkt 1 i pkt 2 rozporządzenia.

Zgodnie z częścią A pkt III ppkt 1 załącznika do rozporządzenia, system informatyczny służący do przetwarzania danych osobowych zabezpiecza się w szczególności przed działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego.

Przeprowadzona kontrola wykazała, że system informatyczny o nazwie „Ramzes” nie został zabezpieczony przed działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego, co stanowi naruszenie wskazanego przepisu załącznika do rozporządzenia. Należy także podnieść, że ze złożonych w odpowiedzi na zawiadomienie o wszczęciu postępowania administracyjnego wyjaśnień oraz załączonych dowodów nie wynika, aby Spółdzielnia podjęła działania mające na celu przywrócenie w tym zakresie stanu zgodnego z prawem.

Jednocześnie, na podstawie złożonych przez Prezesa Zarządu Spółdzielni oraz członka zarządu Spółdzielni pisemnych wyjaśnień oraz przedstawionych pozostałych dowodów, należy stwierdzić, że pozostałe uchybienia w procesie przetwarzania danych osobowych, stanowiące przedmiot postępowania, zostały usunięte, tj.:

1. Zaprzestano pozyskiwania nazwiska rodzowego matki od osób zatrudnionych w Spółdzielni.
2. Utworzone zostały dla dwóch osób odrębne identyfikatory wraz z hasłami dostępu do systemu Windows i programu płac.

Stosownie do art. 105 § 1 Kodeksu postępowania administracyjnego, gdy postępowanie z jakiegokolwiek przyczyny stało się bezprzedmiotowe, organ administracji publicznej wydaje decyzję o jego umorzeniu. W toku postępowania usunięte zostały pozostałe uchybienia w procesie przetwarzania danych osobowych, stanowiące przedmiot postępowania i dlatego w tym zakresie należało je 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.

