



**GENERALNY INSPEKTOR
OCHRONY DANYCH
OSOBOWYCH**

Michał Serzycki

Warszawa, dnia 16 kwietnia 2009 r.

DIS/DEC – 307/13545/09

dot. DIS-K-421/2/09

D E C Y Z J A

Na podstawie art. 104 § 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 6, art. 22 w związku z art. 26 ust. 1 pkt 1, art. 31 ust. 1 i ust. 2, art. 36 ust. 1 i 2 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.), § 4 i § 5 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), częścią A pkt II ust. 1, pkt III ppkt 2, 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 Spółdzielnię Mieszkaniową

I. Nakazuję Spółdzielni Mieszkaniowej usunięcie uchybień w procesie przetwarzania danych osobowych, poprzez:

- 1. Zaprzestanie pozyskiwania od osób zainteresowanych przystąpieniem w poczet członków Spółdzielni Mieszkaniowej danych dotyczących: zawodu, stanu cywilnego, roku urodzenia, daty i miejsca urodzenia, informacji o miejscu pracy i zajmowanym stanowisku, numerze książeczki mieszkaniowej, pozyskanych za pomocą „Deklaracji przystąpienia do Spółdzielni”, w terminie od dnia, w którym niniejsza decyzja stanie się ostateczna.**
- 2. Usunięcie danych osobowych członków Spółdzielni Mieszkaniowej dotyczących: zawodu, stanu cywilnego, roku urodzenia, daty i miejsca urodzenia, informacji o miejscu pracy**

i zajmowanym stanowisku, numeru książeczki mieszkaniowej, pozyskanych za pomocą „Deklaracji przystąpienia do Spółdzielni”, w terminie 2 miesięcy od dnia, w którym niniejsza decyzja stanie się ostateczna.

3. Wskazanie w umowie rozliczeniowej zawartej przez Spółdzielnię Mieszkaniową w dniu 21 czerwca 2000 r. z X zakresu przetwarzania przez X, danych osobowych członków Spółdzielni oraz osób niebędących członkami Spółdzielni a posiadających tytuł prawny do lokalu, w terminie 30 dni od dnia, w którym niniejsza decyzja stanie się ostateczna.

4. Zabezpieczenie dokumentacji składającej się na teczkę lokalu w taki sposób, aby dane osobowe osób, które w przeszłości posiadały tytuł prawny do danego lokalu, nie były dostępne osobom nieupoważnionym, tj. osobom, którym aktualnie przysługuje tytuł prawny do lokalu, w terminie 14 dni od dnia, w którym niniejsza decyzja stanie się ostateczna.

5. Zapewnienie, aby hasło służące do uwierzytelnienia użytkownika w systemie informatycznym o nazwie „Y” składało się co najmniej z 8 znaków, zawierało małe i wielkie litery oraz cyfry lub znaki specjalne i było zmieniane nie rzadziej niż co 30 dni, w terminie 14 dni od dnia, w którym niniejsza decyzja stanie się ostateczna.

6. Zapewnienie, aby komputer, na którym jest zainstalowany system informatyczny o nazwie „Y” został zabezpieczony przed utratą danych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej, w terminie 14 dni od dnia, w którym niniejsza decyzja stanie się ostateczna.

7. Zapewnienie, aby dane osobowe członków Spółdzielni i osób niebędących członkami a posiadających tytuł prawny do lokalu przetwarzane w systemie informatycznym o nazwie „Y”, zostały zabezpieczone poprzez wykonywanie kopii zapasowych zbiorów danych oraz programów służących do przetwarzania danych, w terminie 14 dni od dnia, w którym niniejsza decyzja stanie się ostateczna.

8. Opracowanie i wdrożenie dokumentacji opisującej sposób przetwarzania danych osobowych oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, tj. polityki bezpieczeństwa i instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, spełniającej wymogi określone § 4 i § 5 powołanego rozporządzenia, w terminie 30 dni od dnia, w którym niniejsza decyzja stanie się ostateczna.

U z a s a d n i e n i e

Inspektorzy upoważnieni przez Generalnego Inspektora Ochrony Danych Osobowych, przeprowadzili kontrolę (sygn. akt DIS-K-421/2/09) w Spółdzielni Mieszkaniowej 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 również 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 również rozporządzeniem. W toku kontroli odebrano od pracowników Spółdzielni 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 Prezesa 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. Przetwarzaniu danych osobowych członków Spółdzielni, dotyczących zawodu, stanu cywilnego, roku urodzenia, daty i miejsca urodzenia, informacji o miejscu pracy i zajmowanym stanowisku, numeru książeczki mieszkaniowej, pozyskanych za pomocą formularzy „Deklaracji przystąpienia do Spółdzielni”, z naruszeniem art. 26 ust. 1 pkt 1 ustawy.
2. Nieokreśleniu w umowie rozliczeniowej zawartej przez Spółdzielnię w dniu 21 czerwca 2000 r. z X zakresu przetwarzania przez X danych osobowych członków Spółdzielni oraz osób niebędących członkami Spółdzielni a posiadających tytuł prawny do lokalu (art. 31 ust. 1 i 2 ustawy).
3. Niezabezpieczeniu dokumentacji składającej się na teczkę lokalu w taki sposób, aby dane osobowe osób, które w przeszłości posiadały tytuł prawny do danego lokalu, nie były dostępne osobom nieupoważnionym, tj. osobom, którym aktualnie przysługuje tytuł prawny do lokalu (art. 36 ust. 1 ustawy).
4. Niezapewnieniu, aby hasło służące do uwierzytelnienia użytkownika w systemie informatycznym o nazwie „Y” składało się co najmniej z 8 znaków, zawierało małe i wielkie litery oraz cyfry lub znaki specjalne i było zmieniane nie rzadziej niż co 30 dni (art. 36 ust. 1 ustawy w związku z częścią A pkt II ust. 1 i pkt IV ust. 2 oraz częścią B pkt VIII załącznika do rozporządzenia).
5. Niezapewnieniu, aby komputer, na którym jest zainstalowany system informatyczny o nazwie „Y” został zabezpieczony przed utratą danych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej (art. 36 ust. 1 ustawy w związku z częścią A pkt III ppkt 2 załącznika do rozporządzenia).

6. Niezapewnieniu, aby dane osobowe członków Spółdzielni i osób niebędących członkami a posiadających tytuł prawny do lokalu przetwarzane w systemie informatycznym o nazwie „Y”, zostały zabezpieczone poprzez wykonywanie kopii zapasowych zbioru danych (art. 36 ust. 1 ustawy w związku z częścią A pkt IV ust. 3 załącznika do rozporządzenia).

7. Nieopracowaniu i niewdrożeniu dokumentacji opisującej sposób przetwarzania danych osobowych oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, tj. polityki bezpieczeństwa i instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, spełniających wymogi określone § 4 i § 5 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 (DIS-K-421/2/09/7190), 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. Pomimo to, Spółdzielnia nie złożyła wyjaśnień oraz nie przedstawiła dowodów potwierdzających usunięcie wskazanych uchybień.

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

1. Zgodnie z treścią art. 26 ust. 1 pkt 1 ustawy, administrator danych przetwarzający dane powinien dołożyć szczególnej staranności w celu ochrony interesów osób, których dane dotyczą, a w szczególności jest obowiązany zapewnić, aby dane te były przetwarzane zgodnie z prawem.

Natomiast zgodnie z art. 16 § 1 ustawy z dnia 16 września 1982 r. Prawo spółdzielcze (Dz. U. z 2003 r., Nr 188, poz. 1848 z późn. zm.), warunkiem przyjęcia na członka spółdzielni jest złożenie deklaracji. Deklaracja powinna być złożona w formie pisemnej. Podpisana przez przystępującego do spółdzielni deklaracja powinna zawierać jego imię, nazwisko oraz miejsce zamieszkania, (...), a także inne dane przewidziane w statucie. Z kolei zgodnie z § 10 pkt 2 Statutu Spółdzielni, deklaracja powinna zawierać dane osoby ubiegającej się o członkostwo w zakresie: imię, nazwisko oraz miejsce zamieszkania.

W toku kontroli ustalono, iż w Spółdzielni opracowano formularz „Deklaracji przystąpienia do Spółdzielni”, który wypełniają osoby zainteresowane przystąpieniem w

poczet członków Spółdzielni. Za pomocą ww. formularza, oprócz danych wymienionych w art. 16 § 1 ustawy Prawo spółdzielcze, pozyskiwane są również dane osobowe dotyczące: zawodu, stanu cywilnego, roku urodzenia, daty i miejsca urodzenia, informacji o miejscu pracy i zajmowanym stanowisku, numerze książki mieszkaniowej. Ww. dane nie zostały wymienione w § 10 pkt 2 Statutu Spółdzielni.

W związku z powyższym należy uznać, iż pozyskiwanie przez Spółdzielnię danych dotyczących zawodu, stanu cywilnego, roku urodzenia, daty i miejsca urodzenia, informacji o miejscu pracy i zajmowanym stanowisku, numeru książki mieszkaniowej, za pomocą formularzy „Deklaracji przystąpienia do Spółdzielni”, skutkuje przetwarzaniem danych osobowych z naruszeniem powołanego art. 26 ust. 1 pkt 1 ustawy.

2. Zgodnie z art. 31 ust. 1 ustawy, administrator danych może powierzyć innemu podmiotowi, w drodze umowy zawartej na piśmie, przetwarzanie danych. Natomiast zgodnie z art. 31 ust. 2 ustawy, podmiot, któremu powierzono przetwarzanie danych może je przetwarzać wyłącznie w zakresie i celu przewidzianym w umowie.

W toku kontroli ustalono, że Spółdzielnia w dniu 21 czerwca 2000 r. zawarła umowę rozliczeniową z X. Z treści przedmiotowej umowy wynika, że została ona zawarta w celu rozliczania przez X kosztów zużycia energii cieplnej i innych kosztów eksploatacyjnych w nieruchomościach zarządzanych przez Spółdzielnię. Jak ustalono w umowie, o której mowa powyżej nie został określony zakres przetwarzania danych osobowych członków Spółdzielni oraz osób niebędących członkami Spółdzielni a posiadających tytuł prawny do lokalu. Zatem ww. umowa nie spełnia wymogów, o których mowa w art. 31 ust. 1 i ust. 2 ustawy.

3. Zgodnie z art. 36 ust. 1 ustawy, administrator danych jest obowiązany zastosować środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności powinien zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, zabranieniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem.

W toku kontroli ustalono, że w Spółdzielni dla każdego lokalu zakładana jest odrębnateczka lokalu, w której gromadzone są dokumenty związane z użytkowaniem tego lokalu od momentu jego zasiedlenia, tj. m. in. akty notarialne, składane deklaracje, wymiary opłat i inna korespondencja prowadzona z członkami Spółdzielni i osobami niebędącymi członkami a posiadającymi tytuł prawny do lokalu. Dokumentacja przechowywana w każdej z teczek lokalowych dotyczy wszystkich osób, które posiadały lub posiadają tytuł prawny do danego lokalu i zawiera ich dane osobowe. W przypadku, gdy aktualny właściciel lokalu chce skorzystać z prawa wglądu do teczki dotyczącej swojego lokalu ma możliwość zapoznania się z dokumentacją dotyczącą użytkowania

tego lokalu przez poprzedniego właściciela (właścicieli), tym samym ma dostęp do danych osobowych tej osoby (osób).

Z uwagi na powyższe należy uznać, że Spółdzielnia nie zabezpiecza należycie dokumentacji zawierającej dane osobowe osób, które w przeszłości posiadały tytuł prawny do danego lokalu, ponieważ wyżej opisany sposób przechowywania umożliwia dostęp do niej osobom nieupoważnionym, tj. osobom, którym aktualnie przysługuje tytuł prawny do lokalu.

3.1. Zgodnie z częścią A pkt IV ust. 3 załącznika do rozporządzenia, dane osobowe przetwarzane w systemie informatycznym zabezpiecza się przez wykonywanie kopii zapasowych zbiorów danych oraz programów służących do przetwarzania danych.

W toku kontroli ustalono, że dane osobowe członków Spółdzielni i osób niebędących członkami a posiadających tytuł prawny do lokalu, przetwarzane w systemie informatycznym o nazwie „Y” nie są zabezpieczone przez wykonywanie kopii zapasowych zbioru danych.

3.2 Zgodnie z częścią A pkt II ust. 1 załącznika do rozporządzenia, w systemie informatycznym służącym do przetwarzania danych osobowych stosuje się mechanizmy kontroli dostępu do tych danych. Natomiast zgodnie z częścią A pkt IV ust. 2 załącznika do rozporządzenia, w przypadku, gdy do uwierzytelniania użytkowników używa się hasła, jego zmiana powinna następować nie rzadziej niż co 30 dni. Stosownie do części B pkt VIII załącznika do rozporządzenia, hasło to powinno się składać co najmniej z 8 znaków, zawierających małe i wielkie litery oraz cyfry lub znaki specjalne.

W toku kontroli ustalono, że hasło do systemu informatycznego o nazwie „Y” jest puste. Jednakże z uwag, jakie Spółdzielnia złożyła do protokołu kontroli wynika, że wprowadzono hasło umożliwiające uruchomienie komputera i systemu informatycznego o nazwie „Y”. Z ww. wyjaśnień nie wynika jednak, czy wprowadzone hasło spełnia wymogi rozporządzenia, tj. czy zmiana tego hasła następuje nie rzadziej niż co 30 dni i czy hasło to składa się co najmniej z 8 znaków, zawierających małe i wielkie litery oraz cyfry lub znaki specjalne.

3.3. Zgodnie z częścią A pkt III, ppkt 2 załącznika do rozporządzenia, system informatyczny służący do przetwarzania danych osobowych zabezpiecza się, w szczególności przed: utratą danych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej.

W toku kontroli ustalono, że komputer, na którym jest zainstalowany system informatyczny o nazwie „Y” nie jest zabezpieczony przed utratą danych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej.

4. 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, zwana dalej „instrukcją”. Zgodnie z ust. 2, dokumentację, o której mowa w § 1 pkt 1, prowadzi się w formie pisemnej. Zgodnie z ust. 3, dokumentację, o której mowa w § 1 pkt 1, wdraża administrator danych.

Zgodnie z § 4 rozporządzenia, polityka bezpieczeństwa, o której mowa w § 3 ust. 1, zawiera w szczególności:

- 1) wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe;
- 2) wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych;
- 3) opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi;
- 4) sposób przepływu danych pomiędzy poszczególnymi systemami;
- 5) określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych.

Natomiast 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 w Spółdzielni nie jest prowadzona dokumentacja przetwarzania danych, która spełniałaby wymagania, o których mowa w § 4 i § 5 rozporządzenia.

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.

Wytwórca informacji:

Bogusława Pilec

Dyrektor

Departamentu Inspekcji Biura GIODO

dn. 14 kwietnia 2009 r.

Rodzaj instytucji – Mieszkalnictwo

Zagadnienie – Zabezpieczenie danych, powierzenie przetwarzania