



**GENERALNY INSPEKTOR
OCHRONY DANYCH
OSOBOWYCH**

Michał Serzycki

Warszawa, dnia 23 lutego 2010 r.

DIS/DEC-189/7691/10

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. 36, art. 37, art. 38, art. 39 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 2 i § 7 ust. 3 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. 2 lit. a, częścią A pkt III ust. 1 i ust. 2, częścią A pkt IV ust. 2 i ust. 3, częścią B pkt VIII załącznika do ww. rozporządzenia, po przeprowadzeniu postępowania administracyjnego w sprawie przetwarzania danych osobowych przez Okręgowy Zarząd [...] Polskiego Związku Działkowców, zwany dalej również OZ [...] PZD,

I. Nakazuję Okręgowemu Zarządowi [...] Polskiego Związku Działkowców, usunięcie uchybień w procesie przetwarzania danych osobowych poprzez:

- 1. Zabezpieczenie systemu informatycznego o nazwie „A”, służącego do przetwarzania danych osobowych pracowników OZ [...] PZD, przed działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego, w terminie 30 dni od dnia, w którym niniejsza decyzja stanie się ostateczna.**

2. Zapewnienie, aby dla każdego użytkownika systemu informatycznego o nazwie „B”, służącego do przetwarzania danych osobowych członków Polskiego Związku Działkowców, rejestrowany był odrębny identyfikator, w terminie 30 dni od dnia, w którym niniejsza decyzja stanie się ostateczna.
3. Zabezpieczenie kopią zapasową danych osobowych przetwarzanych w systemie informatycznym o nazwie „B”, w terminie 30 dni od dnia, w którym niniejsza decyzja stanie się ostateczna.
4. Zapewnienie, aby system informatyczny o nazwie „B”, zapewniał odnotowanie identyfikatora użytkownika wprowadzającego dane do systemu, w terminie 3 miesięcy od dnia, w którym niniejsza decyzja stanie się ostateczna.
5. Zapewnienie, aby system informatyczny o nazwie „A” zapewniał sporządzenie i wydrukowanie raportu zawierającego w powszechnie zrozumiałej formie informacje dotyczące daty pierwszego wprowadzenia danych do systemu i identyfikatora użytkownika wprowadzającego ww. dane, w terminie 3 miesięcy od dnia, w którym niniejsza decyzja stanie się ostateczna.
6. Zapewnienie, aby system informatyczny o nazwie „B” zapewniał sporządzenie i wydrukowanie raportu zawierającego w powszechnie zrozumiałej formie informacje dotyczące identyfikatora użytkownika wprowadzającego dane do systemu, w terminie 3 miesięcy 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 w OZ[...] PZD, kontrole zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych sygn. [...] i [...], 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 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, skontrolowano systemy informatyczne oraz dokonano oględzin pomieszczeń, w których odbywa się przetwarzanie danych osobowych. Stan faktyczny został szczegółowo opisany w protokołach kontroli, które zostały podpisane przez osoby uprawnione do reprezentacji OZ [...] PZD.

Na podstawie tak zgromadzonego materiału dowodowego ustalono, że w procesie przetwarzania danych osobowych OZ [...] PZD, jako administrator danych, naruszył przepisy o ochronie danych osobowych. Uchybienia te polegały na:

1. Niezabezpieczeniu systemów informatycznych o nazwach: „A” i „B” przed utratą danych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej (art. 36 ust. 1 ustawy w związku z częścią A pkt III ust. 2 załącznika do rozporządzenia).

2. Niezabezpieczeniu systemu informatycznego o nazwie „A” przed działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego (art. 36 ust. 1 ustawy w związku z częścią A pkt III ust. 1 załącznika do rozporządzenia).

3. Niezapewnieniu, aby dla każdego użytkownika systemu informatycznego o nazwie „B” rejestrowany był odrębny identyfikator (art. 36 ust. 1 ustawy w związku z częścią A pkt II ust. 2 lit. a załącznika do rozporządzenia).

4. Niezapewnieniu, aby zmiana haseł używanych do uwierzytelniania użytkowników w systemach informatycznych o nazwach: „A” i „B”, następowała nie rzadziej niż co 30 dni (art. 36 ust. 1 ustawy w związku z częścią A pkt IV ust. 2 załącznika do rozporządzenia).

5. Niezabezpieczeniu kopią zapasową danych osobowych przetwarzanych w systemie informatycznym o nazwie „B” (art. 36 ust. 1 ustawy w związku z częścią A pkt IV ust. 3 załącznika do rozporządzenia).

6. Niezapewnieniu, aby hasło używane do uwierzytelnienia użytkownika w systemie informatycznym o nazwie „B” składało się co najmniej z 8 znaków, zawierało małe i wielkie litery oraz cyfry lub znaki specjalne (art. 36 ust. 1 ustawy w związku z częścią B pkt VIII załącznika do rozporządzenia).

7. 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).

8. Niewyznaczeniu administratora bezpieczeństwa informacji (art. 36 ust. 3 ustawy).

9. Nienadaniu osobom dopuszczonym do przetwarzania danych osobowych upoważnień do przetwarzania ww. danych (art. 37 ustawy).

10. Niezapewnieniu, aby system informatyczny o nazwie „B” umożliwiał odnotowanie identyfikatora użytkownika, który wprowadził dane osobowe do systemu (art. 38 ustawy w związku z § 7 ust. 1 pkt 2 rozporządzenia).

11. Niezapewnieniu, aby systemy informatyczne o nazwach: „A” i „B”, zapewniały sporządzenie i wydrukowanie raportu zawierającego w powszechnie zrozumiałej formie informacje dotyczące identyfikatora użytkownika wprowadzającego dane do systemu informatycznego oraz

niezapewnieniu, aby system informatyczny o nazwie „A”, zapewniał sporządzenie i wydrukowanie raportu zawierającego w powszechnie zrozumiałej formie informacje dotyczące daty pierwszego wprowadzenia danych do systemu (art. 38 ustawy w związku z § 7 ust. 3 rozporządzenia).

12. Braku ewidencji osób upoważnionych do przetwarzania danych osobowych (art. 39 ustawy).

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

W odpowiedzi na zawiadomienie o wszczęciu postępowania administracyjnego Prezes OZ [...] PZD w piśmie z dnia [...] stycznia 2010 r. złożył wyjaśnienia, w których poinformował między innymi, że:

1. W imieniu administratora danych występuje Prezes OZ [...] PZD.
2. Opracowano politykę bezpieczeństwa i instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.
3. Nadzór nad przestrzeganiem postanowień polityki bezpieczeństwa i instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych został powierzony Dyrektorowi [...] i [...] OZ [...] PZD.
4. Osobom dopuszczonym do przetwarzania danych osobowych nadano stosowne upoważnienia.
5. Opracowano ewidencję osób upoważnionych do przetwarzania danych osobowych.
6. Zakupiono urządzenia zabezpieczające systemy informatyczne o nazwach: „A” i „B”, przed utratą danych na skutek awarii zasilania bądź zakłóceń z sieci zasilającej.
7. Zmodyfikowano hasła służące do uwierzytelniania użytkownika w systemie informatycznym o nazwie „B” w ten sposób, iż ww. hasła składają się z dziesięciu znaków, zawierają duże i małe litery oraz cyfry.
8. Podjęto działania mające na celu:
 - zabezpieczenie systemu informatycznego o nazwie „A” przed działaniem oprogramowania umożliwiającego nieuprawniony dostęp ww. systemu,
 - wprowadzenie odrębnego identyfikatora dla każdego z użytkowników systemu informatycznego o nazwie „B”,
 - wprowadzenie zmiany hasła w użytkowanych systemach informatycznych nie rzadziej niż co 30 dni.
9. W systemie informatycznym o nazwie „A” przetwarzane są dane w zakresie imienia i nazwiska oraz dane liczbowe. Dostosowanie ww. systemu do wymogów zawartych w

przepisach o ochronie danych osobowych w obecnej sytuacji finansowej OZ [...] PZO nie jest możliwe ze względu na koszty jakie wiązałyby się z modyfikacją ww. systemu. Jednocześnie wskazano, iż usuwanie uchybień w procesie przetwarzania danych osobowych będzie realizowane w miarę posiadanych środków, z zastrzeżeniem, iż usunięcie ww. uchybień, ze względów finansowych, nie może być zrealizowane bezzwłocznie. Ponadto, ze względu na trudną sytuację finansową niemożliwe jest usunięcie uchybienia w procesie przetwarzania danych osobowych dotyczącego niezabezpieczenia kopią zapasową danych osobowych przetwarzanych w systemie informatycznym o nazwie „B”. W celu wykonywania kopii zapasowych niezbędny jest zakup urządzenia służącego jako serwer lub odpowiedniego oprogramowania. W chwili obecnej OZ [...] PZD nie dysponuje środkami na wskazany cel.

Ponadto, do pism Dyrektora OZ [...] PZD z dnia [...] stycznia 2010 r. i z dnia [...] lutego 2010 r., załączono: kopię zarządzenia Prezesa OZ [...] PZD w sprawie ustalenia polityki bezpieczeństwa przetwarzania danych osobowych i instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w OZ [...] PZD wraz z załącznikami, kopię przykładowego wpisu do ewidencji osób upoważnionych do przetwarzania danych osobowych oraz kopię przykładowego upoważnienia 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 częścią A pkt III ust. 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.

W toku czynności kontrolnych ustalono, że system informatyczny o nazwie „A” nie jest zabezpieczony przed działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego. Zgodnie z wyjaśnieniami Prezesa OZ[...] PZD, zawartymi w piśmie z dnia [...] stycznia 2010 r., podjęto działania mające na celu usunięcie wskazanego uchybienia. Należy jednak wskazać, iż samo podjęcie wyżej wskazanych działań, nie może być uznane jako przywrócenie stanu zgodnego z prawem.

Zgodnie z częścią A pkt II ust. 2 lit. a załącznika do rozporządzenia, jeżeli dostęp do danych przetwarzanych w systemie informatycznym posiadają co najmniej dwie osoby, wówczas zapewnia się, aby w systemie tym rejestrowany był dla każdego użytkownika odrębny identyfikator.

W toku czynności kontrolnych ustalono, że dostęp do systemu informatycznego o nazwie „B” posiadają dwie osoby. W ww. systemie nie zapewniono, aby dla każdego użytkownika

rejestrowany był odrębny identyfikator. Zgodnie z wyjaśnieniami Prezesa OZ [...] PZD, zawartymi w piśmie z dnia [...] stycznia 2010 r., podjęto działania mające na celu usunięcie powyższego uchybienia. Należy jednak wskazać, iż również w tym przypadku samo podjęcia działań zmierzających do usunięcia wskazanego uchybienia w procesie przetwarzania danych osobowych, nie może być uznane jako przywrócenie stanu zgodnego z prawem.

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 czynności kontrolnych ustalono, że dane osobowe przetwarzane w systemie informatycznym o nazwie „B” nie są zabezpieczone przez wykonywanie kopii zapasowych zbiorów danych oraz programów służących do przetwarzania danych. W wyjaśnieniach Prezesa OZ [...] PZD z dnia [...] stycznia 2010 r. wskazano, iż ze względu na trudną sytuację finansową OZ [...] PZD niemożliwe jest usunięcie ww. uchybienia w procesie przetwarzania danych osobowych, gdyż w celu wykonywania kopii zapasowych niezbędny jest zakup urządzenia służącego jako serwer lub odpowiedniego oprogramowania. Należy wskazać, iż powyższe wyjaśnienia nie zasługują na uwzględnienie, ponieważ omawiane uchybienie może zostać usunięte bez ponoszenia nadmiernych kosztów, poprzez wykonywanie kopii zapasowych na dysku delegowanego w tym celu komputera lub na nośnikach informatycznych.

Zgodnie z § 7 ust. 1 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 identyfikatora użytkownika wprowadzającego dane osobowe do systemu, chyba, że dostęp do systemu informatycznego i przetwarzanych w nim danych posiada wyłącznie jedna osoba.

W toku czynności kontrolnych ustalono, że system informatyczny o nazwie „B” nie zapewnia odnotowania identyfikatora użytkownika, który wprowadził dane osobowe do systemu, a dostęp do ww. systemu informatycznego posiadają dwie osoby.

Zgodnie z § 7 ust. 3 rozporządzenia, dla każdej osoby, której dane osobowe są przetwarzane w systemie informatycznym, system zapewnia sporządzenie i wydrukowanie raportu zawierającego w powszechnie zrozumiałej formie informacje, o których mowa w § 7 ust. 1 rozporządzenia.

W toku czynności kontrolnych ustalono, że systemy informatyczne o nazwach „A” i „B” nie zapewniają sporządzenia i wydrukowania raportu zawierającego w powszechnie zrozumiałej formie informacji dotyczących identyfikatora użytkownika wprowadzającego dane do systemu informatycznego. Ponadto ustalono, że system informatyczny o nazwie „A” nie zapewnia

sporządzenia i wydrukowania raportu zawierającego w powszechnie zrozumiałej formie informacji dotyczących daty pierwszego wprowadzenia danych do systemu. Zgodnie z wyjaśnieniami Prezesa OZ [...] PZD, zawartymi w piśmie z dnia [...] stycznia 2010 r., dostosowanie systemu informatycznego o nazwie „A”, do wymogów zawartych w przepisach o ochronie danych osobowych w obecnej sytuacji finansowej OZ [...] PZO nie jest możliwe ze względu na koszty jakie wiązałyby się z modyfikacją ww. systemu. Jednocześnie wskazano, iż usuwanie uchybień w procesie przetwarzania danych osobowych będzie realizowane w miarę posiadanych środków. Mając na uwadze powyższe wyjaśnienia wyznaczono trzymiesięczny termin na usunięcie w tym zakresie uchybień w procesie przetwarzania danych osobowych.

Jednocześnie, na podstawie złożonych przez OZ [...] PZD dowodów, należy stwierdzić, że pozostałe uchybienia w procesie przetwarzania danych osobowych stanowiące przedmiot postępowania zostały usunięte, tj.:

1. Zabezpieczono systemy informatyczne o nazwach: „A” i „B” przed utratą danych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej.
2. Zapewniono, aby zmiana haseł używanych do uwierzytelniania użytkowników w systemach informatycznych o nazwach: „A” i „B”, następowała nie rzadziej niż co 30 dni.
3. Zapewniono, aby hasło używane do uwierzytelnienia użytkownika w systemie informatycznym o nazwie „B” składało się co najmniej z 8 znaków, zawierało małe i wielkie litery oraz cyfry lub znaki specjalne.
4. Opracowano i wdrożono politykę bezpieczeństwa i instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.
5. Postanowiono, że obowiązki administratora bezpieczeństwa informacji wykonywane będą przez Prezesa OZ [...] PZD.
6. Osobom dopuszczonym do przetwarzania danych osobowych nadano stosowne upoważnienia.
7. Opracowano ewidencję osób upoważnionych do przetwarzania danych osobowych.

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.