GENERALNY INSPEKTOR OCHRONY DANYCH OSOBOWYCH
Michał Serzycki

Warszawa, dnia 30 października 2009 r.

DIS/DEC-
Dot. DIS-K-421/141/09

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 pkt 6 oraz art. 22 w związku z art. 26 ust. 1 pkt 1, art. 31 ust. 1, art. 36. ust. 1 i ust. 2, art. 37, 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.), § 3 ust. 1, i § 7 ust. 1 pkt 1 pkt 2, § 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. 1 i ust. 2 lit. a i b, częścią A pkt IV ust. 3 i ust. 4 załącznika do ww. rozporządzenia, po przeprowadzeniu postępowania administracyjnego w sprawie przetwarzania danych osobowych przez A, B i Wspólnicy Sp. j. z siedzibą w (…),

I. Nakazuję A, B i Wspólnicy Sp. j. z siedzibą w (…), usunięcie uchybień w procesie przetwarzania danych poprzez:

1. **Usunięcie danych osobowych pracowników zawartych w kwestionariuszach osobowych obejmujących nazwisko rodowe matki pracownika w terminie 7 dni od dnia, w którym niniejsza decyzja stanie się ostateczna.**
2. **Zaprzestanie zbierania danych osobowych pracowników zawartych w kwestionariuszach osobowych obejmujących nazwisko rodowe matki pracownika w terminie od dnia, w którym niniejsza decyzja stanie się ostateczna.**

3. **Zawarcie z Panią X prowadzącą działalność gospodarczą pod nazwą „ALA” z siedzibą w(…), umowy powierzenia przetwarzania danych osobowych w terminie 30 dni od dnia, w którym niniejsza decyzja stanie się ostateczna.**
4. **Opracowanie dokumentacji opisującej sposób przetwarzania danych osobowych oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych, tj. polityki bezpieczeństwa i instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w terminie 30 dni od dnia, w którym niniejsza decyzja stanie się ostateczna.**
5. **Nadanie upoważnień do przetwarzania danych osobowych osobom dopuszczonym do przetwarzania danych osobowych w terminie 7 dni od dnia, w którym niniejsza decyzja stanie się ostateczna.**
6. **Opracowanie ewidencji osób upoważnionych do przetwarzania danych osobowych w terminie 7 dni od dnia, w którym niniejsza decyzja stanie się ostateczna..**
7. **Zapewnienie aby system informatyczny służący do przetwarzania danych osobowych (plik o nazwie „urlop.xls”) zapewniał odnotowanie daty pierwszego wprowadzenia danych do systemu w terminie 30 dni od dnia, w którym niniejsza decyzja stanie się ostateczna.**
8. **Zapewnienie aby system informatyczny służący do przetwarzania danych osobowych (plik o nazwie „urlop.xls”) zapewniał odnotowanie identyfikatora użytkownika wprowadzającego dane do systemu w terminie 30 dni od dnia, w którym niniejsza decyzja stanie się ostateczna.**
9. **Zapewnienie aby system informatyczny służący do przetwarzania danych osobowych (plik o nazwie „urlop.xls”) zapewniał sporządzenie i wydrukowanie raportu zawierającego w powszechnie zrozumiałej formie informacje dotyczące daty pierwszego wprowadzenia danych do systemu i identyfikatora użytkownika wprowadzającego ww. dane.**
10. **Zapewnienie aby system informatyczny służący do przetwarzania danych osobowych (plik o nazwie „urlop.xls”) rejestrował dla każdego użytkownika odrębny identyfikator, a dostęp do danych był możliwy wyłącznie po wprowadzeniu identyfikatora i dokonaniu uwierzytelnienia.**

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 A, B i Wspólnicy Sp. j. z siedzibą w (…), zwanej dalej Spółką, kontrolę zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych (sygn.

kontroli 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 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 od pracownika Spółki i jednego ze wspólników Spółki 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 osobę upoważnioną do reprezentacji Spółki.

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

1. Przetwarzaniu danych osobowych pracowników Spółki wykraczających poza zakres danych osobowych wskazany w art. 22^1 § 1 i 2 ustawy z dnia 26 czerwca 1974 r. Kodeks pracy (tekst jednolity: Dz. U. z 1998 r. Nr 21, poz. 94 z późn. zm.), których obowiązek podania nie wynika z odrębnych przepisów prawa, tj. danych dotyczących nazwiska rodowego matki pracownika (art. 26 ust. 1 pkt 1 ustawy).
2. Niezawarciu z podmiotem, któremu Spółka powierzyła przetwarzanie danych osobowych umowy powierzenia przetwarzania danych (art. 31 ust. 1 ustawy).
3. Niezabezpieczeniu bieżącą kopią zapasową danych przetwarzanych w systemie informatycznym (pliku o nazwie „urlop.xls”); niezabezpieczeniu wcześniejszych kopii zapasowych przed nieuprawnionym przejęciem, modyfikacją, uszkodzeniem lub zniszczeniem; nieusunięciu wcześniejszych kopii zapasowych po ustaniu ich użyteczności (art. 36. ust. 1 ustawy w związku z częścią A pkt IV ust. 3 i ust. 4 załącznika do rozporządzenia).
4. 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).
5. Nienadaniu osobom przetwarzającym dane osobowe upoważnień do przetwarzania ww. danych (art. 37 ustawy).
6. Braku ewidencji osób upoważnionych do przetwarzania danych osobowych (art. 39 ustawy).
7. Niezapewnieniu aby system informatyczny (plik o nazwie „urlop.xls”) umożliwiał odnotowanie daty pierwszego wprowadzenia danych do systemu (§ 7 ust. 1 pkt 1 rozporządzenia).
8. Niezapewnieniu aby system informatyczny (plik o nazwie „urlop.xls”) umożliwiał odnotowanie identyfikatora użytkownika wprowadzającego dane do systemu (§ 7 ust. 1 pkt 2 rozporządzenia).

9. Niezapewnieniu aby system informatyczny (plik o nazwie „urlop.xls”) umożliwiał sporządzenie i wydrukowanie raportu zawierającego w powszechnie zrozumiałej formie informacje dotyczące daty pierwszego wprowadzenia danych i identyfikatora użytkownika wprowadzającego dane do systemu (§ 7 ust. 3 rozporządzenia).
10. Umożliwieniu dostępu do systemu informatycznego (pliku o nazwie „urlop.xls”) bez wprowadzenia identyfikatora i dokonania uwierzytelnienia (część A pkt II ust. 1 i ust. 2 lit. a i b załącznika do rozporządzenia.

W związku z powyższym, w dniu 23 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 wspólnik Spółki Pan Y w pismach z dnia 28 września 2009 r. i 19 października 2009 r. złożył wyjaśnienia, w których poinformował między innymi, że:

1. Spółka zobowiązała się do usunięcia danych dotyczących nazwiska rodowego matki pracowników Spółki.

2. Pełnomocnictwo udzielone Pani X uznawane jest w Spółce za podstawę powierzenia ww. osobie przetwarzania danych osobowych pracowników Spółki bez konieczności zawarcia umowy w tym zakresie.

3. Kopia zapasowa pliku „urlop.xls” została odnaleziona, zaktualizowana i zabezpieczona.

4. Nieprawdą jest, iż w toku kontroli nie został udostępniony zakres obowiązków służbowych pracownika upoważnionego do przetwarzania danych osobowych, gdyż inspektorzy upoważnieni przez Generalnego Inspektora Ochrony Danych Osobowych do przeprowadzenia czynności kontrolnych otrzymali do wglądu umowę o pracę ww. pracownika. Zawarty we wskazanej umowie o pracę zakres obowiązków sformułowany jako „czynności kadrowe” jest równoznaczny z upoważnieniem do przetwarzania danych osobowych, a okres upoważnienia jest tożsamy z okresem trwania umowy o pracę.

Ponadto w nadesłanych wyjaśnieniach wskazano, że plik „urlop.xls” jest programem opracowanym przez Spółkę na jej wyłączny użytek, nie jest objęty licencjami i nie obsługuje czytników identyfikatorów, w związku z czym zaskoczeniem dla Spółki jest wymóg identyfikacji, sporządzania raportów, czy rejestrowania każdego wejścia do niego. Nadesłane wyjaśnienia zawierały również informacje dotyczące systemu informatycznego wykorzystywanego do przekazywania informacji do Zakładu Ubezpieczeń Społecznych.

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

Zgodnie z art. 26 ust. 1 pkt 1 ustawy, administrator 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 stosownie do art. 22^1 § 1 ustawy z dnia 26 czerwca 1974 r. Kodeks pracy (tekst jednolity: Dz. U. z 1998 r. Nr 21, poz. 94 z późn. zm.) pracodawca ma prawo żądać od osoby ubiegającej się o zatrudnienie podania danych osobowych obejmujących: imię (imiona) i nazwisko, imiona rodziców, datę urodzenia, miejsce zamieszkania (adres do korespondencji), wykształcenie, przebieg dotychczasowego zatrudnienia, a w myśl art. 22^1 § 2 pracodawca ma prawo żądać od pracownika podania, niezależnie od danych, o których mowa w § 1, także: innych danych osobowych pracownika, a także imion i nazwisk oraz dat urodzenia dzieci pracownika, jeżeli podanie takich danych jest konieczne ze względu na korzystanie przez pracownika ze szczególnych uprawnień przewidzianych w prawie pracy, numeru PESEL pracownika nadanego przez Rządowe Centrum Informatyczne Powszechnego Elektronicznego Systemu Ewidencji Ludności (RCI PESEL), zaś stosownie do art. 22^1 § 4 pracodawca może żądać podania innych danych osobowych niż określone w § 1 i 2, jeżeli obowiązek ich podania wynika z odrębnych przepisów. Natomiast art. 22^1 § 5 wskazuje, iż w zakresie nieuregulowanym w § 1- 4 do danych osobowych, o których mowa w tych przepisach, stosuje się przepisy o ochronie danych osobowych.

W toku kontroli ustalono, że w Spółce przetwarzane są dane osobowe pracowników zawarte w kwestionariuszu osobowym. Za pomocą ww. kwestionariusza, wypełnianego przez zatrudnianą osobę, pozyskiwane są między innymi dane dotyczące nazwiska rodowego matki pracownika. W związku z powyższym należy uznać, iż przetwarzanie danych dotyczących nazwiska rodowego matki pracownika jest niezgodne z prawem, gdyż wykracza poza zakres danych osobowych wskazany w art. 22^1 § 1 i 2 Kodeksu pracy, a obowiązek ich podania nie wynika z odrębnych przepisów prawa. Wyjaśnienia złożone prze osobę reprezentującą Spółkę dotyczące planowanego w Spółce usunięcia danych dotyczących nazwiska rodowego matki pracownika nie mają wpływu na rozstrzygnięcia niniejszej decyzji. Należy wskazać, iż sama deklaracja kontrolowanego podmiotu dotycząca usunięcia uchybień w procesie przetwarzania danych osobowych nie jest równoznaczna z usunięciem ww. uchybień.

Zgodnie z art. 31 ust. 1 ustawy, administrator danych może powierzyć innemu podmiotowi, w drodze umowy zawartej na piśmie, przetwarzanie danych.

W toku kontroli ustalono, że w celu prowadzenia obsługi księgowej Spółki dane osobowe pracowników udostępniane są Pani X - księgowej prowadzącej działalność gospodarczą pod nazwą „ALA” z siedzibą w(…).

Ww. przedsiębiorcy udzielone zostało pełnomocnictwo do reprezentacji Spółki przed Urzędem Skarbowym i Zakładem Ubezpieczeń Społecznych we wszystkich sprawach związanych

z prowadzeniem księgowości. Wskazane pełnomocnictwo według wyjaśnień złożonych przez osobę reprezentującą Spółkę uznawane jest w Spółce za podstawę powierzenia przetwarzania danych osobowych pracowników.

Powołane pełnomocnictwo nie stanowi podstawy powierzenia przetwarzania danych, ponieważ ustawa dopuszczając możliwość powierzenia przetwarzania danych osobowych jako podstawę ww. powierzenia w sposób jednoznaczny wskazuje zawarcie umowy w tym zakresie. Należy wskazać, że zgodnie z art. 31 ust. 2 ustawy, podmiot, któremu administrator danych powierzył przetwarzanie danych osobowych może przetwarzać dane wyłącznie w zakresie i celu przewidzianym w umowie. Wobec powyższego tylko umowa zawarta na piśmie, zawierająca zakres i cel w jakim dane będą przetwarzane, może być podstawą powierzenia innemu podmiotowi przetwarzania danych osobowych.

Zgodnie 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.

W toku kontroli ustalono, że w Spółce nie jest prowadzona dokumentacja stanowiąca politykę bezpieczeństwa oraz instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.

Zgodnie z art. 37 ustawy, do przetwarzania danych mogą być dopuszczone wyłącznie osoby posiadające upoważnienie nadane przez administratora danych.

W toku czynności kontrolnych Pan Y (wspólnik Spółki) odmówił udostępnienia zakresu obowiązków służbowych pracowników Spółki, z których (zgodnie
z wyjaśnieniami ww. osoby) wynika upoważnienie do przetwarzania danych. Nie można zgodzić się ze stanowiskiem Pana Y zawartym w piśmie z dnia 28 września 2009 r., iż ww. zakres obowiązków służbowych został w toku kontroli udostępniony, gdyż fakt nieudostępnienia wskazanego zakresu obowiązków został opisany w protokole kontroli podpisanym przez ww. osobę. Ponadto należy wskazać, iż wyjaśnienia Pana Y zgodnie z którymi sformułowanie „czynności kadrowe” jest równoznaczne z upoważnieniem do przetwarzania danych osobowych, a okres upoważnienia jest tożsamy z okresem trwania umowy o pracę, nie poparte żadnym materiałem dowodowym, nie stanowią podstawy do uznania, iż uchybienia w procesie przetwarzania danych osobowych w tym zakresie zostały usunięte.

Zgodnie z art. 39 ustawy, administrator danych prowadzi ewidencję osób upoważnionych do ich przetwarzania, która powinna zawierać: 1) imię i nazwisko osoby upoważnionej, 2) datę

nadania i ustania oraz zakres upoważnienia do przetwarzania danych osobowych, 3) identyfikator, jeżeli dane są przetwarzane w systemie informatycznym.

W toku kontroli ustalono, że Spółka nie prowadzi ewidencji osób upoważnionych do przetwarzania danych osobowych.

Zgodnie z § 7 ust. 1 pkt 1 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.

W toku czynności kontrolnych ustalono, że system informatyczny (plik o nazwie „urlop.xls") nie zapewnia odnotowania daty pierwszego wprowadzenia danych do systemu.

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 dostęp do systemu informatycznego (pliku o nazwie „urlop.xls") posiadają cztery osoby, z których dwie użytkują wskazany system w zakresie wprowadzania i modyfikacji danych. Jak ustalono system informatyczny (plik o nazwie „urlop.xls") nie zapewnia odnotowania identyfikatora użytkownika wprowadzającego dane do systemu.

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 system informatyczny (plik o nazwie „urlop.xls") nie zapewnia sporządzenia i wydrukowania raportu zawierającego w powszechnie zrozumiałej formie informacji, o których mowa w § 7 ust. 1 rozporządzenia, w zakresie dotyczącym daty pierwszego wprowadzenia danych oraz identyfikatora użytkownika wprowadzającego dane do systemu informatycznego.

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 w myśl wymogu, o którym mowa w części A pkt II ust. 2 lit. a i b 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, a dostęp do danych był możliwy wyłącznie po wprowadzeniu identyfikatora i dokonaniu uwierzytelnienia.

W toku czynności kontrolnych ustalono, że dostęp do systemu informatycznego (pliku o nazwie „urlop.xls") posiada w Spółce więcej niż jedna osoba, a ww. dostęp możliwy jest bez wprowadzenia identyfikatora i dokonania uwierzytelnienia.

Ponadto, w nawiązaniu do złożonych przez osobę reprezentującą Spółkę wyjaśnień, z których wynika, że plik „urlop.xls" jest programem opracowanym przez Spółkę na jej wyłączny użytek, nie jest objęty licencjami i nie obsługuje czytników identyfikatorów należy wskazać, iż ww. informacje nie mają wpływu na ocenę obowiązku zapewnienia przez administratora danych aby system informatyczny służący do przetwarzania danych osobowych spełniał wymogi określone w rozporządzeniu. Jednocześnie odnosząc się do złożonych przez osobę reprezentującą Spółkę wyjaśnień należy wskazać, iż system informatyczny wykorzystywany do przekazywania informacji do Zakładu Ubezpieczeń Społecznych nie był objęty zakresem postępowania w sprawie uchybień w procesie przetwarzania danych osobowych przez Spółkę.

Stosowanie do art. 105 § 1 Kodeksu postępowania administracyjnego, gdy postępowanie z jakiejkolwiek 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 jakiejkolwiek 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).

W toku postępowania, poprzez aktualizację i zabezpieczenie kopii zapasowej pliku „urlop.xls", usunięte zostało uchybienie w procesie przetwarzania danych osobowych stanowiące przedmiot postępowania, 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.