



**GENERALNY INSPEKTOR
OCHRONY DANYCH
OSOBOWYCH**

Michał Serzycki

Warszawa, dnia 21 października 2008 r.

DIS/DEC – 671/28142/08

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. 38 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r., Nr 101, poz. 926 z późn. zm.) oraz § 7 ust. 1 pkt 1 i 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), po przeprowadzeniu postępowania administracyjnego w sprawie przetwarzania danych osobowych przez Gimnazjum w L.,

I. Nakazuję Gimnazjum w L., usunięcie uchybień w procesie przetwarzania danych osobowych, poprzez:

1. Zapewnienie, aby system informatyczny o nazwie „A”, w którym przetwarzane są dane osobowe uczniów Szkoły, odnotowywał datę pierwszego wprowadzenia danych do systemu, w terminie 3 miesięcy od dnia, w którym niniejsza decyzja stanie się ostateczna.

2. Zapewnienie, aby system informatyczny o nazwie „B”, w którym przetwarzane są dane osobowe pracowników Szkoły, odnotowywał datę pierwszego wprowadzenia danych do systemu oraz identyfikator użytkownika wprowadzającego dane osobowe do systemu, w terminie 3 miesięcy od dnia, w którym niniejsza decyzja stanie się ostateczna.

3. Zapewnienie, aby system informatyczny o nazwie „A”, w którym przetwarzane są dane osobowe uczniów Szkoły, umożliwiał sporządzenie i wydrukowanie raportu zawierającego datę pierwszego wprowadzenia danych do systemu, w terminie 3 miesięcy od dnia, w którym niniejsza decyzja stanie się ostateczna.

4. Zapewnienie, aby system informatyczny o nazwie „B”, w którym przetwarzane są dane osobowe pracowników Szkoły, umożliwiał sporządzenie i wydrukowanie raportu zawierającego datę pierwszego wprowadzenia danych do systemu oraz identyfikator użytkownika wprowadzającego dane osobowe 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 kontrolę w Gimnazjum w L., zwanym dalej Gimnazjum lub Szkołą, w celu ustalenia zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych (sygn. akt [...]), 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 Gimnazjum 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 Dyrektora Szkoły. Na podstawie tak zgromadzonego materiału dowodowego ustalono, że w procesie przetwarzania danych osobowych, Gimnazjum naruszyło przepisy o ochronie danych osobowych. Uchybienia te polegały na:

1. Pozyskiwaniu na kwestionariuszach osobowych dla pracowników danej dotyczącej nazwiska rodowego matki pracownika Szkoły (art. 26 ust. 1 pkt 1 ustawy).
2. Niezabezpieczeniu systemów informatycznych o nazwach: „C”, „D” służących do przetwarzania danych osobowych, przed utratą danych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej (część A pkt III ppkt 2 załącznika do rozporządzenia).
3. Niezapewnieniu, aby hasła używane do uwierzytelnienia użytkownika w systemach informatycznych o nazwach: „E”, „F”, „G”, „D” były zmieniane nie rzadziej niż co 30 dni (część A pkt IV ust. 2 załącznika do rozporządzenia).
4. Niezapewnieniu, aby system informatyczny o nazwie „A”, w którym przetwarzane są dane osobowe uczniów Szkoły, odnotowywał datę pierwszego wprowadzenia danych do systemu (§ 7 ust. 1 pkt 1 rozporządzenia).
5. Niezapewnieniu, aby system informatyczny o nazwie „B”, w którym przetwarzane są dane osobowe pracowników Szkoły, odnotowywał datę pierwszego wprowadzenia danych do systemu oraz identyfikator użytkownika wprowadzającego dane osobowe do systemu (§ 7 ust. 1 pkt 1 i 2 rozporządzenia).
6. Niezapewnieniu, aby system informatyczny o nazwie „A”, w którym przetwarzane są dane osobowe uczniów Szkoły, umożliwiał sporządzenie i wydrukowanie raportu zawierającego datę pierwszego wprowadzenia danych do systemu (§ 7 ust 3 rozporządzenia).
7. Niezapewnieniu, aby system informatyczny o nazwie „B”, w którym przetwarzane są dane osobowe pracowników Szkoły, umożliwiał sporządzenie i wydrukowanie raportu zawierającego datę pierwszego wprowadzenia danych do systemu oraz identyfikator użytkownika wprowadzającego dane osobowe do systemu (§ 7 ust 3 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 (nr [...]), 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.

W odpowiedzi na powyższe pismo Gimnazjum pismem z dnia [...] sierpnia 2008 r. złożyło wyjaśnienia w sprawie wskazanych uchybień, w których poinformowało, że dane osobowe zawarte w kwestionariuszach osobowych, dotyczące nazwiska rodowego matki pracownika zostały usunięte, natomiast aktualny kwestionariusz osobowy nie wymaga podania przez pracownika przedmiotowej danej. Ponadto w ww. piśmie Szkoła wskazała, iż systemy informatyczne o nazwach: „F”, „D” służące do przetwarzania danych osobowych, zostały obecnie zabezpieczone

przed utratą danych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej. Gimnazjum wyjaśniło również, iż aktualnie hasła używane do uwierzytelnienia użytkownika w systemach informatycznych o nazwach: „E”, „F”, „G”, „D” są zmieniane przez ich użytkowników nie rzadziej niż co 30 dni. Odnosząc się natomiast do uchybień dotyczących systemów informatycznych o nazwach „A” oraz „B” Szkoła w powołanym piśmie poinformowała, iż zwróciła się do [...] Komisji Egzaminacyjnej w sprawie zajęcia przez nią stanowiska dotyczącego systemu o nazwie „A” oraz do Ministerstwa Edukacji Narodowej w sprawie zajęcia stanowiska dotyczącego systemu o nazwie „B”.

Do wskazanych wyjaśnień załączono następujące dowody: wzór aktualnego kwestionariusza osobowego dla pracownika, kserokopia faktury VAT nr [...] za zakup urządzeń [...], kserokopie pism skierowanych do [...] Komisji Egzaminacyjnej oraz do Ministerstwa Edukacji Narodowej.

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

Zgodnie z art. 38 ustawy, administrator danych jest obowiązany zapewnić kontrolę nad tym, jakie dane osobowe, kiedy i przez kogo zostały do zbioru wprowadzone oraz komu są przekazywane.

Natomiast zgodnie z § 7 ust. 1 pkt 1 i 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: 1) daty pierwszego wprowadzenia danych do systemu; 2) identyfikatora użytkownika wprowadzającego dane osobowe do systemu, chyba że dostęp do systemu informatycznego i przetwarzanych w nim danych posiada wyłącznie jedna osoba (...).

Jednocześnie 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, których mowa w ust. 1

W toku czynności kontrolnych ustalono, że system informatyczny o nazwie „A” nie zapewnia odnotowania daty pierwszego wprowadzenia danych do systemu.

Ponadto ustalono, iż system informatyczny o nazwie „B” nie zapewnia odnotowania daty pierwszego wprowadzenia danych do systemu oraz identyfikatora użytkownika wprowadzającego dane osobowe do systemu.

W toku przeprowadzonych czynności kontrolnych ustalono również, że system informatyczny o nazwie „A”, w którym przetwarzane są dane osobowe uczniów Szkoły, nie

zapewnia sporządzenia i wydrukowania raportu zawierającego datę pierwszego wprowadzenia danych do systemu. Natomiast, system informatyczny o nazwie „B”, w którym przetwarzane są dane osobowe pracowników Szkoły, nie zapewnia sporządzenia i wydrukowania raportu zawierającego datę pierwszego wprowadzenia danych do systemu oraz identyfikator użytkownika wprowadzającego dane osobowe do systemu.

Należy zauważyć, iż z brzmienia przepisów ustawy o ochronie danych osobowych i 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, wynika w sposób nie budzący wątpliwości, że to na administratorze danych, spoczywają określone w tych przepisach obowiązki. Administrator danych jest zobowiązany zadbać o to, aby proces przetwarzania danych był zgodny z powołanymi przepisami prawa, w tym, aby systemy informatyczne służące do przetwarzania danych osobowych posiadały wymagane funkcjonalności. W przypadku, gdy administrator danych zobowiązany jest korzystać z narzędzi dostarczonych przez inny podmiot, winien wystąpić do tego podmiotu o zapewnienie, aby odpowiadały one wymogom określonym w przepisach prawa. W piśmie z dnia [...] sierpnia 2008 r. Dyrektor Gimnazjum wskazał, iż wystosowane zostały pisma do odpowiednich podmiotów z prośbą o dokonanie zmian w systemach informatycznych, tak aby spełniały one wymagania określone w przepisach o ochronie danych osobowych. Należy jednak podkreślić, iż samo podjęcie działań w celu usunięcia uchybień nie stanowi podstawy do uznania, że został przywrócony stan zgodny z prawem. Powyższe okoliczności uwzględniono natomiast przy określaniu terminu na dostosowanie ww. systemów do wymogów ustawy i rozporządzenia.

Jednocześnie, na podstawie złożonych przez administratora danych pisemnych wyjaśnień oraz przedstawionych dowodów, należy stwierdzić, że pozostałe uchybienia w procesie przetwarzania danych osobowych, stanowiące przedmiot postępowania, zostały usunięte, tj.: Szkoła usunęła dane dotyczące nazwiska rodzowego matki pracownika pozyskiwane na kwestionariuszach osobowych dla pracowników oraz zaprzestała dalszego ich pozyskiwania; systemy informatyczne o nazwach: „F”, „D” służące do przetwarzania danych osobowych zostały zabezpieczone przed utratą danych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej; hasła używane do uwierzytelnienia użytkownika w systemach informatycznych o nazwach: „E”, „F”, „G”, „D” są zmieniane nie rzadziej niż co 30 dni.

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

beprzedmiotowość 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. S.A./Sz1029/97).

W toku postępowania usunięte zostały pozostałe uchybienia w procesie przetwarzania danych osobowych, stanowiące przedmiot postępowania i dlatego 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.