GENERALNY INSPEKTOR
OCHRONY DANYCH
OSOBOWYCH
Michał Serzycki

Warszawa, dnia 17 października 2008 r.

DIS/DEC - 667/27832/08

dot. […]

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 art. 22 w związku z art. 36 ust. 1 i 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 § 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 III ppkt 2 załącznika powołanego rozporządzenia, po przeprowadzeniu postępowania administracyjnego w sprawie przetwarzania danych osobowych przez Gimnazjum w W.,

nakazuję

Gimnazjum w W., usunięcie uchybień w procesie przetwarzania danych osobowych, poprzez:

1. Zabezpieczenie systemów informatycznych o nazwie „A", „B", „C", „D" służących do przetwarzania danych osobowych oraz danych osobowych przetwarzanych w plikach typu […], przed utratą danych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej, w terminie dwóch tygodni od dnia, w którym niniejsza decyzja stanie się ostateczna.

2. Zapewnienie, aby system informatyczny o nazwie „C" odnotowywał datę pierwszego wprowadzenia danych do systemu, w terminie trzech miesięcy od dnia, w którym niniejsza decyzja stanie się ostateczna.

3. Zapewnienie, aby system informatyczny o nazwie „A" odnotowywał datę pierwszego wprowadzenia danych do systemu, w terminie jednego miesiąca od dnia, w którym niniejsza decyzja stanie się ostateczna.

4. Zapewnienie, aby system informatyczny o nazwie „D" odnotowywał datę pierwszego wprowadzenia danych do systemu, w terminie trzech miesięcy od dnia, w którym niniejsza decyzja stanie się ostateczna.

5. Zapewnienie, aby system informatyczny o nazwie „C" umożliwiał sporządzenie i wydrukowanie raportu zawierającego datę pierwszego wprowadzenia danych do systemu, w terminie trzech miesięcy od dnia, w którym niniejsza decyzja stanie się ostateczna.

6. Zapewnienie, aby system informatyczny o nazwie „A" umożliwiał sporządzenie i wydrukowanie raportu zawierającego datę pierwszego wprowadzenia danych do systemu, w terminie jednego miesiąca od dnia, w którym niniejsza decyzja stanie się ostateczna.

7. Zapewnienie, aby system informatyczny o nazwie „D" umożliwiał sporządzenie i wydrukowanie raportu zawierającego datę pierwszego wprowadzenia danych do systemu, w terminie trzech miesięcy 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 w Gimnazjum w W., zwanym dalej Gimnazjum, 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). W toku kontroli m.in. odebrano od pracowników 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 Gimnazjum. Na podstawie zgromadzonego materiału dowodowego ustalono, że Gimnazjum naruszyło przepisy o ochronie danych osobowych. Uchybienia te polegały na:

1. Nie zabezpieczeniu systemów informatycznych o nazwie „A", „B", „C", „D" oraz danych przetwarzanych w plikach typu […] 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).
2. Nie zapewnieniu, aby system informatyczny o nazwie „C" odnotowywał datę pierwszego wprowadzenia danych do systemu (§ 7 ust. 1 pkt 1 rozporządzenia).
3. Nie zapewnieniu, aby system informatyczny o nazwie „A" odnotowywał datę pierwszego wprowadzenia danych do systemu (§ 7 ust. 1 pkt 1 rozporządzenia).
4. Nie zapewnieniu, aby system informatyczny o nazwie „D" odnotowywał datę pierwszego wprowadzenia danych do systemu (§ 7 ust. 1 pkt 1 rozporządzenia).
5. Nie zapewnieniu, aby system informatyczny o nazwie „C" umożliwiał sporządzenie i wydrukowanie raportu zawierającego datę pierwszego wprowadzenia danych do systemu (§ 7 ust. 3 rozporządzenia).
6. Nie zapewnieniu, aby system informatyczny o nazwie „A" umożliwiał sporządzenie i wydrukowanie raportu zawierającego datę pierwszego wprowadzenia danych do systemu (§ 7 ust. 3 rozporządzenia).
7. Nie zapewnieniu, aby system informatyczny o nazwie „D" umożliwiał sporządzenie i wydrukowanie raportu zawierającego datę pierwszego wprowadzenia danych 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. Pomimo to, Gimnazjum nie złożyło wyjaśnień oraz nie przedstawiło 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 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, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem.

Natomiast 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 czynności kontrolnych ustalono, że systemy informatyczne o nazwie „A", „B", „C", „D" oraz dane przetwarzane w plikach typu […] służące do przetwarzania danych osobowych nie zostały zabezpieczone, przed utratą danych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej.

2. 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 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.

2.1. W toku czynności kontrolnych ustalono, że w systemie informatycznym o nazwie „C" nie jest odnotowywana data pierwszego wprowadzenia danych do systemu.

2.2. W toku czynności kontrolnych ustalono, że w systemie informatycznym o nazwie „A" nie jest odnotowywana data pierwszego wprowadzenia danych do systemu.

2.3. W toku czynności kontrolnych ustalono, że w systemie informatycznym o nazwie „D" nie jest odnotowywana data pierwszego wprowadzenia danych do systemu.

3. 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. 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. l.

3.1. W toku czynności kontrolnych ustalono, że system informatyczny o nazwie „C" nie zapewnia sporządzenia i wydrukowania raportu zawierającego datę pierwszego wprowadzenia danych do systemu.

3.2. W toku czynności kontrolnych ustalono, że system informatyczny o nazwie „A" nie zapewnia sporządzenia i wydrukowania raportu zawierającego datę pierwszego wprowadzenia danych do systemu.

3.3. W toku czynności kontrolnych ustalono, że system informatyczny o nazwie „D" nie zapewnia sporządzenia i wydrukowania raportu zawierającego datę pierwszego wprowadzenia danych do systemu.

W świetle dokonanych ustaleń, 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.