



**GENERALNY INSPEKTOR
OCHRONY DANYCH
OSOBOWYCH**

Michał Serzycki

Warszawa, dnia 14 stycznia 2008 r.

DIS-DEC-12/656/08

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. 26 ust. 1 pkt 2, art. 36 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.) oraz § 3, § 7 ust. 1 pkt 1 i 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), po przeprowadzeniu postępowania administracyjnego w sprawie przetwarzania danych osobowych przez Collegium I.,

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

- 1. Zapewnienie, aby zgoda na przetwarzanie danych osobowych, umieszczona na formularzach deklaracji członkowskich Collegium I., obejmowała również publikowanie danych w internecie, w terminie 14 dni od dnia, w którym niniejsza decyzja stanie się ostateczna.**
- 2. Zapewnienie, aby w zbiorze danych członków Stowarzyszenia (studentów i tutorów) prowadzonym przy pomocy systemu informatycznego o nazwie „A”, była odnotowywana data pierwszego wprowadzenia danych do systemu oraz identyfikator użytkownika**

wprowadzającego dane osobowe do systemu w terminie 30 dni od dnia, w którym niniejsza decyzja stanie się ostateczna.

3. Zapewnienie, aby system informatyczny o nazwie „A”, przy pomocy którego przetwarzane są dane członków Stowarzyszenia i tutorów, zapewniał dla każdej osoby, której dane osobowe są w nim przetwarzane, sporządzenie i wydrukowanie raportu zawierającego w powszechnie zrozumiałej formie informacje, o których mowa w § 7 ust. 1 rozporządzenia, w terminie 30 dni od dnia, w którym niniejsza decyzja stanie się ostateczna.

4. Opracowanie i wdrożenie polityki bezpieczeństwa, w terminie 14 dni od dnia, w którym niniejsza decyzja stanie się ostateczna.

5. Opracowanie i wdrożenie instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, w terminie 14 dni od dnia, w którym niniejsza decyzja stanie się ostateczna.

6. Nadanie upoważnień osobom dopuszczonym do przetwarzania danych, w terminie 14 dni od dnia, w którym niniejsza decyzja stanie się ostateczna.

7. Opracowanie i prowadzenie ewidencji osób upoważnionych do przetwarzania danych osobowych, zawierającej: imię i nazwisko osoby upoważnionej, datę nadania i ustania, zakres upoważnienia do przetwarzania danych osobowych oraz identyfikator, jeżeli dane są przetwarzane w systemie informatycznym, w terminie 14 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 w Collegium I., zwanym dalej również Stowarzyszeniem, 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 członka Zarządu Stowarzyszenia 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 członków Zarządu Stowarzyszenia. Na

podstawie tak zgromadzonego materiału dowodowego ustalono, że w procesie przetwarzania danych osobowych, Stowarzyszenie naruszyło przepisy o ochronie danych osobowych. Uchybienia te polegały na:

1. Niepozyskiwaniu od członków Stowarzyszenia, zgody na publikowanie ich danych osobowych w Internecie (art. 26 ust. 1 pkt 2 ustawy).
2. Niezapewnieniu, aby w zbiorze danych członków Stowarzyszenia (studentów i tutorów) prowadzonym przy pomocy systemu informatycznego o nazwie „A”, była odnotowywana data pierwszego wprowadzenia danych do systemu oraz identyfikator użytkownika wprowadzającego dane osobowe do systemu (§ 7 ust. 1 pkt 1 i 2 rozporządzenia).
3. Niezapewnieniu, aby system informatyczny o nazwie „A”, przy pomocy którego przetwarzane są dane członków Stowarzyszenia i tutorów, zapewniał dla każdej osoby, której dane osobowe są w nim przetwarzane, sporządzenie i wydrukowanie raportu zawierającego w powszechnie zrozumiałej formie informacje, o których mowa w § 7 ust. 1 rozporządzenia (§ 7 ust. 3 rozporządzenia).
4. Nieopracowaniu dokumentacji opisującej sposób przetwarzania danych 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 (art. 36 ust. 2 ustawy oraz § 3 rozporządzenia).
5. Dopuszczeniu do przetwarzania danych osób nieposiadających upoważnień nadanych przez administratora danych (art. 37 ustawy).
6. Nieopracowaniu przez administratora ewidencji osób upoważnionych do przetwarzania danych osobowych (art. 39 ustawy).

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, Stowarzyszenie 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 treścią art. 26 ust. 1 pkt 2 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: zbierane dla oznaczonych, zgodnych z prawem celów i nie poddawane dalszemu przetwarzaniu niezgodnemu z tymi celami, z zastrzeżeniem ust. 2.

Jak ustalono w toku kontroli, na ogólnodostępnej stronie internetowej zamieszczone są imiona i nazwiska członków Stowarzyszenia, a w przypadku członków czynnych, także ich zainteresowania, nazwa uczelni, na której studiują. Fakt publikowania na stronie internetowej danych członków Stowarzyszenia wynika z przyjętej formy działania, misji Stowarzyszenia. Jest to też jedna z form promowania działalności członków Stowarzyszenia. Na formularzach deklaracji członkowskich Collegium I. zbierana jest zgoda na przetwarzanie danych osobowych w celach zgodnych ze statutem organizacji. Stowarzyszenie nie wykazało innej podstawy prawnej do publikowania danych osobowych swoich członków na stronie internetowej. Wobec powyższego należy uznać, że wskazana w deklaracji członkowskiej zgoda na przetwarzanie danych powinna obejmować również publikowanie danych w internecie, bowiem taki cel przetwarzania danych nie mieści się w celach zgodnych ze statutem organizacji.

2. 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: daty pierwszego wprowadzenia danych do systemu, identyfikatora użytkownika wprowadzającego dane osobowe do systemu, chyba że dostęp do systemu informatycznego i przetwarzanych w nim danych posiada wyłącznie jedna osoba.

W zbiorze danych członków Stowarzyszenia (studentów i tutorów) prowadzonym przy pomocy systemu informatycznego o nazwie „A”, nie jest odnotowywana data pierwszego wprowadzenia danych do systemu, ani identyfikator użytkownika wprowadzającego dane osobowe do systemu.

3. 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 ust. 1.

System informatyczny o nazwie „A”, przy pomocy którego przetwarzane są dane członków Stowarzyszenia i tutorów nie zapewnia dla każdej osoby, której dane osobowe są przetwarzane w nim, sporządzenia i wydrukowania raportu zawierającego w powszechnie zrozumiałej formie informacji, o których mowa w § 7 ust. 1 rozporządzenia.

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. Natomiast, zgodnie z ust. 3, dokumentację, o której mowa w § 1 pkt 1, wdraża administrator danych.

W toku czynności kontrolnych ustalono, że w Stowarzyszeniu nie jest prowadzona dokumentacja opisująca sposób przetwarzania danych oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, tj. polityka bezpieczeństwa i instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.

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

W toku czynności kontrolnych ustalono, że do przetwarzania danych dopuszczone zostały osoby nieposiadające upoważnienia nadanego przez administratora danych.

6. Zgodnie art. 39 ustawy Administrator danych prowadzi ewidencję osób upoważnionych do przetwarzania danych osobowych, 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 czynności kontrolnych ustalono, iż nie jest prowadzona ewidencja osób upoważnionych do przetwarzania danych.

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.