GENERALNY INSPEKTOR OCHRONY DANYCH OSOBOWYCH
dr Wojciech R. Wiewiórowski

Warszawa, dnia 13 stycznia 2012 r.

DIS/DEC- 40/12/2282
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, art. 36 ust. 2, art. 36 ust. 3, art. 37, 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.) § 3, § 7 ust. 1 pkt 1 i pkt 2 oraz § 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), a także częścią A pkt IV ust. 2 załącznika do ww. rozporządzenia, po przeprowadzeniu postępowania administracyjnego w sprawie przetwarzania danych osobowych przez S. Sp. z o.o. s. k. ,

nakazuję S. Sp. z o.o. s. k., przywrócenie stanu zgodnego z prawem w procesie przetwarzania danych osobowych, poprzez:

1. Zapewnienie aby zmiana hasła do systemu informatycznego o nazwie „A" (w którym przetwarzane są dane osobowe […]) oraz systemu operacyjnego następowała nie rzadziej niż co 30 dni, w terminie 7 dni od dnia, w którym niniejsza decyzja stanie się ostateczna.

2. Opracowanie w formie pisemnej dokumentacji opisującej sposób przetwarzania danych osobowych 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, w terminie 30 dni od dnia, w którym niniejsza decyzja stanie się ostateczna.

3. Wyznaczenie administratora bezpieczeństwa informacji, nadzorującego przestrzeganie zasad ochrony przetwarzanych danych osobowych, w terminie od dnia, w którym niniejsza decyzja stanie się ostateczna.

4. Nadanie osobom dopuszczonym do przetwarzania danych upoważnień do przetwarzania danych osobowych, w terminie od dnia, w którym niniejsza decyzja stanie się ostateczna.

5. Zapewnienie, aby system informatyczny o nazwie „A" umożliwiał dla każdej osoby, której dane osobowe są przetwarzane w tym systemie informatycznym, odnotowanie daty pierwszego wprowadzenia danych do systemu oraz identyfikatora użytkownika wprowadzającego dane osobowe do systemu, w terminie 60 dni od dnia, w którym niniejsza decyzja stanie się ostateczna.

6. Zapewnienie, aby system informatyczny o nazwie „A", umożliwiał dla każdej osoby, której dane osobowe są przetwarzane w ww. systemie informatycznym, sporządzenie i wydrukowanie raportu zawierającego w powszechnie zrozumiałej formie informacje o dacie pierwszego wprowadzenia danych do systemu oraz identyfikatorze użytkownika wprowadzającego dane osobowe do systemu, w terminie 60 dni od dnia, w którym niniejsza decyzja stanie się ostateczna.

7. Opracowanie ewidencji osób upoważnionych do przetwarzania danych osobowych, w terminie 7 dni od dnia, w którym niniejsza decyzja stanie się ostateczna.

Uzasadnienie

Inspektorzy, upoważnieni przez Generalnego Inspektora Ochrony Danych Osobowych przeprowadzili kontrolę w S. Sp. z o.o. s. k. (dalej: Spółka) w celu ustalenia zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych sygn. […], 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 Spółki 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 Prezesa Zarządu Spółki.

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

1) niezapewnieniu aby zmiana hasła do systemu informatycznego o nazwie „A." oraz systemu operacyjnego następowała nie rzadziej niż co 30 dni (art. 36 ust. 1 ustawy w związku z częścią A pkt IV ust. 2 załącznika do rozporządzenia),

2) nieopracowaniu w formie pisemnej dokumentacji opisującej sposób przetwarzania danych osobowych 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 w związku z § 3 rozporządzenia),

3) niewyznaczeniu administratora bezpieczeństwa informacji, nadzorującego przestrzeganie zasad ochrony przetwarzanych danych osobowych (art. 36 ust. 3 ustawy),

4) nienadaniu osobom dopuszczonym do przetwarzania danych upoważnień do przetwarzania danych osobowych (art. 37 ustawy),

5) niezapewnieniu, aby system informatyczny o nazwie „A." umożliwiał dla każdej osoby, której dane osobowe są przetwarzane w tym systemie informatycznym, odnotowanie daty pierwszego wprowadzenia danych do systemu oraz identyfikatora użytkownika wprowadzającego dane osobowe do systemu (art. 36 ust. 1 ustawy w związku z § 7 ust. 1 pkt 1 i pkt 2 rozporządzenia),

6) niezapewnieniu, aby system informatyczny o nazwie „A.", umożliwiał dla każdej osoby, której dane osobowe są przetwarzane w ww. systemie informatycznym, sporządzenie i wydrukowanie raportu zawierającego w powszechnie zrozumiałej formie informacje o dacie pierwszego wprowadzenia danych do systemu oraz identyfikatorze użytkownika wprowadzającego dane osobowe do systemu (art. 36 ust. 1 ustawy w związku z § 7 ust. 3 rozporządzenia),

7) nieopracowaniu ewidencji osób upoważnionych do przetwarzania danych osobowych (art. 39 ustawy).

W piśmie z dnia […] grudnia 2011 r. sygn. […], stanowiącym zawiadomienie o wszczęciu postępowania administracyjnego w przedmiotowej sprawie, Spółka została poinformowana o prawie czynnego udziału w każdym stadium postępowania, a przed wydaniem decyzji wypowiedzenia się co do zebranych dowodów i materiałów oraz zgłoszonych żądań. Spółka nie skorzystała z prawa złożenia wyjaśnień oraz nie przesłała dowodów mogących potwierdzić usunięcie uchybień stwierdzonych w toku kontroli.

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

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 IV ust. 2 załącznika do rozporządzenia, w przypadku gdy do uwierzytelnienia użytkowników używa się hasła, jego zmiana następuje nie rzadziej niż co 30 dni.

W toku czynności kontrolnych ustalono, że hasło do systemu informatycznego o nazwie „A." (w którym przetwarzane są dane osobowe […]) oraz systemu operacyjnego nie jest zmieniane.

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.

W toku kontroli ustalono, iż w Spółce nie opracowano polityki bezpieczeństwa oraz instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.

Zgodnie z art. 36 ust. 3 ustawy, administrator danych wyznacza administratora bezpieczeństwa informacji, nadzorującego przestrzeganie zasad ochrony, o których mowa w ust. 1, chyba że sam wykonuje te czynności.

W Spółce nie został wyznaczony administrator bezpieczeństwa informacji.

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

W toku kontroli ustalono, iż osobom dopuszczonym w Spółce do przetwarzania danych osobowych nie zostały nadane upoważnienia do ich przetwarzania.

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 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: 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 toku czynności kontrolnych ustalono, iż system informatyczny o nazwie „A.” nie zapewnia odnotowania daty pierwszego wprowadzenia danych do systemu oraz identyfikatora użytkownika wprowadzającego dane osobowe do systemu.

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, o których mowa w ust. 1.

W toku przedmiotowej kontroli ustalono, że system informatyczny o nazwie „A.” nie zapewnia sporządzenia i wydrukowania raportu zawierającego w powszechnie zrozumiałej formie informacje, o dacie pierwszego wprowadzenia danych osobowych do systemu oraz identyfikatorze użytkownika wprowadzającego dane osobowe do systemu.

Zgodnie z art. 39 ust. 1 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.

Mając powyższe na uwadze, w tym stanie prawnym i faktycznym, Generalny Inspektor Ochrony Danych Osobowych rozstrzygnął, jak w sentencji.

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. W razie niewykonania decyzji w terminie zostanie wobec podmiotu zobowiązanego do jej wykonania wszczęte postępowanie egzekucyjne na podstawie przepisów ustawy z dnia 17 czerwca 1966 r. o postępowaniu egzekucyjnym w administracji (Dz. U. z 2005 r. Nr 229, poz. 1954, z późn. zm.).