



**GENERALNY INSPEKTOR
OCHRONY DANYCH
OSOBOWYCH**

dr Wojciech R. Wiewiórowski

Warszawa, dnia 20 października 2011 r.

DIS/DEC- 883/50669/11

dot. DIS-K-421/107/11

DECYZJA

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 i art. 22 w zw. z art. 36 ust. 1 i art. 41 ust. 2 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926, z późn. zm.) oraz częścią B pkt IX załącznika do 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 Policję.

I. Nakazuję Policji, usunięcie uchybienia w procesie przetwarzania danych osobowych, poprzez zabezpieczanie środkami ochrony kryptograficznej nośników CD/DVD, na których przetwarzane są dane osobowe uczestników imprez masowych, wobec których został wydany prawomocny wyrok o ukaraniu za przestępstwo albo wykroczenie, popełnione w związku z imprezą masową, przekazywanych z Policji do X, tj. poza obszar, o którym mowa w § 4 pkt 1 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), w terminie od dnia, w którym niniejsza decyzja stanie się ostateczna.

II. W pozostałym zakresie postępowanie umarzam.

Uzasadnienie

Inspektorzy, upoważnieni przez Generalnego Inspektora Ochrony Danych Osobowych przeprowadzili w Policji, kontrolę zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych (sygn. DIS-K-421/107/11), tj. ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, 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 Policji ustne wyjaśnienia, skontrolowano systemy informatyczne służące do przetwarzania danych osobowych oraz dokonano oględzin pomieszczeń, w których odbywa się przetwarzanie danych osobowych. Stan faktyczny został szczegółowo opisany w protokole kontroli, który został podpisany przez przedstawiciela Policji.

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

- 1) niezabezpieczeniu środkami ochrony kryptograficznej nośników CD/DVD, na których przetwarzane są dane osobowe uczestników imprez masowych, wobec których został wydany prawomocny wyrok o ukaraniu za przestępstwo albo wykroczenie, popełnione w związku z imprezą masową, przekazywanych z Policji do firmy X (dalej: Spółka), tj. poza obszar, o którym mowa w § 4 pkt 1 rozporządzenia (art. 36 ust. 1 ustawy w związku z częścią B pkt IX załącznika do rozporządzenia),
- 2) niedokonaniu aktualizacji zbioru danych o nazwie „Policyjny Rejestr Imprez Masowych” - księga rejestrowa nr (art. 41 ust. 2 ustawy).

W piśmie z dnia 06 września 2011 r. (sygn. DIS-K-421/107/11/42238), stanowiącym zawiadomienie o wszczęciu postępowania administracyjnego w przedmiotowej sprawie, Policja 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.

W odpowiedzi na zawiadomienie o wszczęciu postępowania administracyjnego przedstawiciel Policji, pismem z dnia 16 września 2011 r. złożył wyjaśnienia, w których poinformował, iż:

1) nośniki CD/DVD zawierające dane o uczestnikach imprez masowych, wobec których został wydany prawomocny wyrok o ukaraniu za przestępstwo albo wykroczenie, popełnione w związku z imprezą masową są przekazywane uprawnionym do ich otrzymania podmiotom, w obszarze przetwarzania danych wskazanym w Polityce Bezpieczeństwa Policji. Przekazywanie danych odbywa się na terenie budynku Policji w sposób zapewniający poufność i integralność tych danych. Przekazywanie danych następuje wyłącznie pomiędzy imiennie wskazanymi osobami (upoważniony funkcjonariusz Policji i upoważniony pracownik Spółki.). Ponadto wskazano, iż z chwilą przekazania danych obowiązek zabezpieczenia danych przechodzi na ten podmiot, który w taki sposób otrzymał dane osobowe,

2) dokonano aktualizacji zbioru danych o nazwie „Policyjny Rejestr Imprez Masowych” - księga rejestrowa nr (dowód: kopia powołanego zgłoszenia aktualizacyjnego).

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, zabranieniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem. Natomiast zgodnie z częścią B pkt IX załącznika do rozporządzenia, urządzenia i nośniki zawierające dane osobowe, o których mowa w art. 27 ust. 1 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, przekazywane poza obszar, o którym mowa w § 4 pkt 1 rozporządzenia, zabezpiecza się w sposób zapewniający poufność i integralność tych danych.

W toku kontroli ustalono, że w Policji nie zastosowano niezbędnych środków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych określone w rozporządzeniu. Jak ustalono przekazywane na nośnikach CD/DVD dane osobowe uczestników imprez masowych, wobec których został wydany prawomocny wyrok o ukaraniu za przestępstwo albo wykroczenie, popełnione w związku z imprezą masową (tzw. zakazy wstępu na imprezę masową) z Policji do Spółki nie są zabezpieczone środkami ochrony kryptograficznej.

Należy podnieść, iż podejmowane przez administratora danych środki, o których mowa w art. 36 ust. 1 ustawy, mają przeciwdziałać nie tylko ukierunkowanym i zamierzonym działaniom ze strony osób trzecich, lecz także działaniom przypadkowym lub nawet związanym z siłą wyższą; chodzi tu zatem zarówno na przykład o celowe „wykradanie” danych, jak i o ich uszkodzenie wskutek wadliwości stosowanego sprzętu lub oprogramowania, nieuwagi pracowników (por. J. Barta, P. Fajgielski, R. Markiewicz, Ochrona Danych Osobowych, Komentarz, Wyd. 4, Kraków 2007, str. 600). Dlatego też administrator danych jest obowiązany monitorować i oceniać

zmieniające się zagrożenia w związku z przetwarzaniem danych osobowych i odpowiednio do zachodzących zmian wykorzystywać, uwzględniając osiągnięcia nauki i techniki, środki techniczne i organizacyjne (por. A. Drozd, Ustawa o ochronie danych osobowych, Komentarz, Wzory pism i przepisy, Wyd. 2, Warszawa 2006, str. 245). Jednocześnie podejmując decyzję w zakresie stosowanych środków zabezpieczenia danych, administrator danych powinien uwzględnić, przede wszystkim jakie kategorie danych osobowych są przetwarzane.

Zgodnie z § 6 ust. 1 rozporządzenia, uwzględniając kategorie przetwarzanych danych oraz zagrożenia wprowadza się poziomy bezpieczeństwa przetwarzania danych osobowych w systemie informatycznym: 1) podstawowy; 2) podwyższony; 3) wysoki.

Przy rozróżnieniu wskazanych poziomów wzięto pod uwagę dwa kryteria: rodzaj danych oraz dostęp urządzeń informatycznych do sieci publicznej. Przyjęto przy tym zasadę, iż należy zastosować poziom ochrony przynajmniej taki, jaki wynika z kryteriów poddawanych ocenie, co oznacza, że można zastosować poziom wyższy. W toku czynności kontrolnych ustalono, iż na nośnikach CD/DVD przetwarzane są dane, o których mowa w art. 27 ust. 1 ustawy, tj. dane osobowe uczestników imprez masowych, wobec których został wydany prawomocny wyrok o ukaraniu za przestępstwo albo wykroczenie, popełnione w związku z imprezą masową. Wobec powyższego w analizowanym przypadku winien być zastosowany co najmniej poziom podwyższony.

W części B pkt IX załącznika do rozporządzenia wskazano, iż urządzenia i nośniki zawierające dane osobowe, o których mowa w art. 27 ust. 1 ustawy, przekazywane poza obszar, o którym mowa w § 4 pkt 1 rozporządzenia, zabezpiecza się w sposób zapewniający poufność i integralność tych danych.

Należy podnieść, iż w przedmiotowej sprawie dane osobowe przekazywane są poza obszar, o którym mowa w § 4 pkt 1 rozporządzenia. Nie ma znaczenia w tym przypadku fakt, iż nośniki z danymi osobowymi przekazywane są fizycznie na terenie budynku Policji osobie upoważnionej do ich odebrania. Nośniki z danymi osobowymi faktycznie przekazywane są przez Policję poza obszar wskazany w § 4 pkt 1 rozporządzenia podmiotowi, który otrzymuje je w sposób niezabezpieczony. Niezabezpieczenie nośników z ww. danymi przez Policję stwarza zagrożenie dla poufności oraz integralności tych danych. Przez integralność danych zgodnie z § 2 pkt 8 rozporządzenia, rozumie się właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany. Natomiast przez poufność danych zgodnie z § 2 pkt 10 rozporządzenia, rozumie się właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym podmiotom.

Z uwagi na powyższe zasadne jest aby nośniki zawierające dane osobowe zostały zabezpieczone przed ich przekazaniem podmiotowi zewnętrznemu, tj. Spółka w celu zapewnienia poufności i integralności danych osobowych.

Jednocześnie w analizowanym przypadku nie można przenieść całego ryzyka utraty danych

na podmiot, który je otrzymał w sposób niezabezpieczony zwłaszcza, że przekazanie danych miało miejsce na terenie Policji.

Reasumując, Policja powinna zabezpieczać środkami ochrony kryptograficznej nośniki CD/DVD, na których przetwarzane są dane osobowe uczestników imprez masowych, wobec których został wydany prawomocny wyrok o ukaraniu za przestępstwo albo wykroczenie, popełnione w związku z imprezą masową, przekazywane do Spółki tj. poza obszar, o którym mowa w § 4 pkt 1 rozporządzenia.

Jednocześnie, na podstawie przedstawionych wyjaśnień i pozostałych dowodów w niniejszej sprawie, należy stwierdzić, że pozostałe uchybienie w procesie przetwarzania danych osobowych, stanowiące przedmiot postępowania, zostało usunięte, tj. dokonano aktualizacji zbioru danych o nazwie „Policyjny Rejestr Imprez Masowych” (księga rejestrowa nr ...).

Stosownie do art. 105 § 1 Kodeksu postępowania administracyjnego, gdy postępowanie z jakiegokolwiek przyczyny stało się bezprzedmiotowe, organ administracji publicznej wydaje decyzję o jego umorzeniu. Jak stwierdził Naczelny Sąd Administracyjny w uzasadnieniu wyroku z dnia 19 listopada 2001 r. (sygn. akt II SA 2702/00): „(...) skoro w toku prowadzonego (...) postępowania administracyjnego zniesiony został stan naruszenia prawa, którego miało dotyczyć rozstrzygnięcie, to postępowanie stało się bezprzedmiotowe”.

W związku z tym, że w toku postępowania usunięte zostało pozostałe uchybienie w procesie przetwarzania danych osobowych, stanowiące przedmiot postępowania, w tym zakresie należało je umorzyć.

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.).

Otrzymują:

1. gen. insp. Andrzej Matejuk

Komendant Główny Policji

ul. Puławska 148/150

02-624 Warszawa

2. A/a