GENERALNY INSPEKTOR OCHRONY DANYCH OSOBOWYCH

dr Edyta Bielak – Jomaa

Warszawa, dnia 15 grudnia 2015 r.

DIS/DEC-954/15/105865

dot. […]

D E C Y Z J A

Na podstawie art. 104 § 1 i 105 § 1 ustawy z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego (Dz. U. z 2013 r. poz. 267 z późn. zm.), art. 12 pkt 2, 18 ust. 1 pkt 1 i art. 22 w związku z art. 36 ust. 1 i 39 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2014 r. poz. 1182 z późn. zm.) oraz częścią A pkt IV ust. 2 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 A. Sp. z o.o.

I. Nakazuję A. Sp. z o.o. usunięcie uchybień w procesie przetwarzania danych osobowych poprzez zapewnienie, aby zmiana hasła do systemu informatycznego „Windows 7”, w którym przetwarzane są dane osobowe osób wnioskujących o wydanie dokumentów związanych z przebiegiem zatrudnienia na podstawie przechowywanej przez Spółkę dokumentacji osobowej i płacowej następowała nie rzadziej niż co 30 dni, w terminie 2 miesięcy od dnia, w którym niniejsza decyzja stanie się ostateczna.

II. W pozostałym zakresie postępowanie umarzam.

]Uzasadnienie

Upoważnieni przez Generalnego Inspektora Ochrony Danych Osobowych inspektorzy przeprowadzili w Spółce, kontrolę 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 2014 r. poz. 1182 z późn. zm.), zwaną dalej: „ustawą", i 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". Zakresem kontroli objęto przetwarzanie przez A. Sp. z o.o., zwaną dalej: „Spółką", danych osobowych zawartych w dokumentacji osobowej i płacowej dotyczącej pracowników, dla których pracodawcą nie jest Spółką, lecz inne podmioty, w tym Z […].

W toku kontroli odebrano od pełnomocnika Spółki ustne wyjaśnienia, skontrolowano systemy informatyczne oraz dokonano oględzin pomieszczeń, w których odbywa się przetwarzanie danych osobowych. Stan faktyczny szczegółowo opisano w protokole kontroli, który został podpisany przez pełnomocnika Spółki.

Na podstawie tak zgromadzonego materiału dowodowego ustalono, że Spółka, jako administrator danych, naruszyła przepisy o ochronie danych osobowych. Uchybienia polegały na:

1. Niezapewnieniu, aby zmiana hasła do systemu informatycznego „Windows 7", w którym przetwarzane są dane osobowe osób wnioskujących o wydanie dokumentów związanych z przebiegiem zatrudnienia na podstawie przechowywanej przez Spółkę dokumentacji osobowej i płacowej następowała nie rzadziej niż co 30 dni (część A pkt IV ust. 2 rozporządzenia).

2. Niespełnieniu przez administratora danych wymogów, o których mowa w art. 39 ust. 1 ustawy w zakresie, w jakim prowadzona ewidencja osób upoważnionych nie zawierała identyfikatora użytkownika w systemie informatycznym, którym posługuje się on podczas uwierzytelniania w systemie informatycznym, będący jednocześnie identyfikatorem indeksującym wykonane przez niego operacje.

W związku z powyższym, Generalny Inspektor Ochrony Danych Osobowych wszczął z urzędu postępowanie administracyjne w niniejszej sprawie w celu wyjaśnienia okoliczności sprawy. W piśmie z dnia […] (znak: […]) zawiadamiającym 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.

W odpowiedzi na zawiadomienie o wszczęciu postępowania administracyjnego, pełnomocnik Spółki pismem z dnia […] złożył wyjaśnienia, w których poinformował, iż:

1. W dniu […] wydano zarządzenie nr […], mocą którego Krajowy Dyrektor ds. Systemów Informatycznych został zobowiązany do wprowadzenia w Spółce rozwiązań organizacyjnych i technicznych mających na celu spełnienie obowiązku zmiany co 30 dni hasła dostępu do systemu operacyjnego Windows wykorzystywanego w Spółce przez osoby przetwarzające dane osobowe w jej systemach informatycznych. Spółka wskazała także, iż z uwagi na fakt, że system operacyjny Windows nie jest administrowany w Polsce, zaś w Grupie A. obowiązuje wymóg zmiany hasła dostępu do tego systemu co 3 miesiące, dostosowanie się przez Spółkę do wymogu zmiany hasła z częstotliwością nie rzadziej niż co 30 dni wynikającego z załącznika do rozporządzenia rodzi konieczność dokonania odpowiednich uzgodnień i podjęcia decyzji przez administratora systemu operacyjnego Windows w Grupie A., co wymaga odpowiednio długiego czasu. Dlatego też Spółka ustaliła 3 miesięczny termin wykonania ww. zarządzenia.

2. Na mocy ww. zarządzenia nr […] Spółka podjęła decyzję o wprowadzeniu zmian w stosowanej ewidencji osób upoważnionych do przetwarzania danych osobowych poprzez wprowadzenie oprócz dotychczasowego, nowego identyfikatora w postaci służbowego adresu poczty elektronicznej pracownika oraz loginu Active Directory, które są unikalne dla każdego pracownika i którym osoby te posługują się podczas uwierzytelniania w systemach informatycznych Spółki, także w celu przetwarzania danych osobowych. Spółka wskazała, iż odpowiednie zmiany w prowadzonej ewidencji osób upoważnionych zostały już dokonane, załączając do pisma z dnia […] dowody potwierdzające dokonanie ww. zmian.

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

Zgodnie z częścią A pkt IV ust. 2 załącznika do rozporządzenia, w przypadku, gdy do uwierzytelniania użytkowników używa się hasła, jego zmiana następuje nie rzadziej, niż co 30 dni.

W toku kontroli ustalono, iż hasło do systemu operacyjnego „Windows 7” na komputerze Specjalisty ds. administracji personalnej, z którego możliwy jest dostęp do pliku w formacie „Excel” o nazwie „[…]” (zawierającego imię i nazwisko osoby kierującej podanie o dostęp do dotyczącej jej dokumentacji osobowej i płacowej, w tym uzyskanie stosownych zaświadczeń stworzonych w oparciu o ww. dokumentację, zakres żądania, datę wysyłki skanu podania do P. Sp. z o.o. oraz adnotację, na której fakturze żądanie zostało rozliczone), a także do wiadomości e-mail od osób kierujących ww. podanie w formie elektronicznej, jest zmieniane rzadziej niż co 30 dni.

Z pisma powołanego powyżej pisma Spółki z dnia […] oraz dołączonego do niego zarządzenia nr […] z dnia […] wynika, iż modyfikacja częstotliwości zmiany hasła nastąpi nie wcześniej niż w terminie 3 miesięcy od dnia wydania ww. zarządzenia.

Powyższe daje podstawę do uznania, iż Spółka nadal nie stosuje wymogów określonych w części A pkt IV ust. 2 załącznika do rozporządzenia, naruszając tym samym wskazaną normę.

Uwzględniając jednak wyjaśnienia Spółki, iż system informatyczny Windows nie jest administrowany w Polsce, konieczność dokonania odpowiednich uzgodnień z administratorem ww. systemu informatycznego, które mają na celu przywróceniu stanu zgodnego z prawem, a także datę wydania zarządzenia nr […] Generalny Inspektor Ochrony Danych Osobowych wyznaczył dwumiesięczny termin wykonania niniejszej decyzji w tym zakresie.

Jednocześnie, na podstawie przedstawionych wyjaśnień i innych dowodów w niniejszej sprawie, należy stwierdzić, że kolejne z uchybień w procesie przetwarzania danych osobowych, stanowiące przedmiot niniejszego postępowania administracyjnego, zostało usunięte. Prowadzona w Spółce ewidencja osób upoważnionych do przetwarzania danych osobowych spełnia bowiem wymogi, o których mowa w art. 39 ust. 1 ustawy.

Stosownie do art. 105 § 1 Kodeksu postępowania administracyjnego, gdy postępowanie z jakiejkolwiek 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”. Ponadto przesłanką umorzenia postępowania na podstawie art. 105 § 1 k.p.a. jest bezprzedmiotowość postępowania „z jakiejkolwiek przyczyny”, czyli każdej przyczyny powodującej brak jednego z elementów materialnego stosunku prawnego w odniesieniu do jego strony podmiotowej lub przedmiotowej (wyrok NSA z 21 stycznia 1999 r. SA/Sz. 1029/97).

W związku z tym, że w toku postępowania usunięte zostało wyżej wymienione uchybienie w procesie przetwarzania danych osobowych, postępowanie w tym zakresie należało umorzyć.

Wobec powyższego, 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.