GENERALNY INSPEKTOR OCHRONY DANYCH OSOBOWYCH

dr Wojciech R. Wiewiórowski

Warszawa, dnia 17 lipca 2014 r.

DIS/DEC-678/55376/14

dot. […]

D E C Y Z J A

Na podstawie art. 104 § 1 i art. 105 § 1 ustawy z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego (Dz. U. z 2013 r., poz. 267), art. 12 pkt 2, art. 18 ust. 1 pkt 1 i art. 22 w związku z art. 36 ust. 3 i art. 39 ust. 1 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r., Nr 101, poz. 926 z późn. zm.), § 4 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 art. 174d ust. 1 ustawy z dnia 16 lipca 2004 r. Prawo telekomunikacyjne (Dz. U. Nr 171, poz. 1800 z późn. zm.), po przeprowadzeniu postępowania administracyjnego w sprawie przetwarzania danych osobowych przez P. S.A.,

I. Nakazuję P. S.A. usunięcie uchybień w procesie przetwarzania danych osobowych poprzez zmodyfikowanie systemu informatycznego o nazwie „[…]" (wykorzystywanego do przetwarzania danych osobowych abonentów), w taki sposób, aby zapewniał sporządzenie i wydrukowanie raportu zawierającego w powszechnie zrozumiałej formie informacje, o których mowa w § 7 ust. 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 3 miesięcy od dnia, w którym niniejsza decyzja stanie się ostateczna.

II. W pozostałym zakresie postępowanie umarzam.

U z a s a d n i e n i e

Inspektorzy upoważnieni przez Generalnego Inspektora Ochrony Danych Osobowych przeprowadzili kontrolę w P. S.A., zwanej dalej „Spółką”, 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”. Kontrola dotyczyła zawiadomienia z dnia […] listopada 2013 r., o naruszeniu danych osobowych, które zostało zgłoszone Generalnemu Inspektorowi Ochrony Danych Osobowych przez Spółkę, na podstawie art. 174a ust. 1 ustawy z dnia 16 lipca 2004 r. Prawo telekomunikacyjne (Dz. U. Nr 171, poz. 1800 z późn. zm.). 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 pełnomocnika Spółki.

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

1. Niewyznaczeniu administratora bezpieczeństwa informacji (36 ust. 3 ustawy).
2. Nieprowadzeniu ewidencji osób upoważnionych do przetwarzania danych osobowych (art. 39 ust. 1 ustawy).
3. Niezawarciu w obowiązującym w Spółce dokumencie o nazwie „Polityka bezpieczeństwa danych osobowych” wykazu budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe; wykazu zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych; opisu struktury zbiorów danych wskazującego zawartość poszczególnych pól informacyjnych i powiązania między nimi; sposobu przepływu danych pomiędzy poszczególnymi systemami (§ 4 rozporządzenia).
4. Niezapewnianiu przez system informatyczny o nazwie „[…]”, wykorzystywany do przetwarzania danych osobowych, sporządzenia i wydrukowania raportu zawierającego w powszechnie zrozumiałej formie informacje, o których mowa w § 7 ust. 1 rozporządzenia (§ 7 ust. 3 rozporządzenia).

5. Nieprowadzeniu rejestru naruszeń danych osobowych, o którym mowa w art. 174d ust. 1 Prawa telekomunikacyjnego.

W związku z powyższym, w dniu […] maja 2014 r. Generalny Inspektor Ochrony Danych Osobowych wszczął z urzędu postępowanie administracyjne w niniejszej sprawie w celu wyjaśnienia okoliczności sprawy (sygn. pisma […]).

W odpowiedzi na zawiadomienie o wszczęciu postępowania administracyjnego wyznaczony w Spółce administrator bezpieczeństwa informacji pismami z dnia […] czerwca 2014 r., nr […], i z dnia […] czerwca 2014 r., nr […], złożył wyjaśnienia, w których poinformował, że:

1. W Spółce na podstawie uchwały nr […] Zarządu Spółki z dnia […] maja 2014 r. powołany został administrator bezpieczeństwa informacji.
2. Sporządzono ewidencję osób upoważnionych do przetwarzania danych osobowych, a osobom dopuszczonym do przetwarzania danych nadano upoważnienia do ich przetwarzania.
3. Uzupełniono dokument o nazwie „Polityka bezpieczeństwa danych osobowych" o wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe; wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych; opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi; sposób przepływu danych pomiędzy poszczególnymi systemami.
4. Trwają prace nad „uzgodnieniem" raportu zawierającego w powszechnie zrozumiałej formie wymagane informacje, dla każdej osoby, której dane osobowe są przetwarzane w systemie informatycznym o nazwie „[…]".
5. Sporządzono wzór rejestru naruszeń danych osobowych.

Ponadto, do ww. pism wyznaczony w Spółce administrator bezpieczeństwa informacji załączył dowody mające 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 § 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.

Przeprowadzona kontrola wykazała, że system informatyczny o nazwie „[…]" nie zapewnia dla każdej osoby, której dane osobowe są przetwarzane w systemie informatycznym,

sporządzenia i wydrukowania raportu zawierającego w powszechnie zrozumiałej formie informacje, o których mowa w § 7 ust. 1 rozporządzenia, co stanowi naruszenie ww. przepisu rozporządzenia.

W pismach stanowiących odpowiedź na zawiadomienie o wszczęciu postępowania administracyjnego wyznaczony w Spółce administrator bezpieczeństwa informacji poinformował o trwających pracach nad „uzgodnieniem" raportu zawierającego w powszechnie zrozumiałej formie wymagane informacje, dla każdej osoby, której dane osobowe są przetwarzane w systemie informatycznym o nazwie „[…]". Należy podkreślić, że podjęcie tych działań nie może jednak stanowić podstawy do uznania, że w ww. zakresie przywrócony został stan zgodny z prawem. Administrator danych nadal nie zapewnia bowiem możliwości sporządzenia i wydrukowania raportu, o którym mowa w nakazie niniejszej decyzji, a jedynie podjął kroki w celu realizacji tego obowiązku.

Jednocześnie, na podstawie złożonych przez wyznaczonego w Spółce administratora bezpieczeństwa informacji pisemnych wyjaśnień oraz innych przedstawionych dowodów, należy stwierdzić, że pozostałe uchybienia w procesie przetwarzania danych osobowych, stanowiące przedmiot postępowania, zostały usunięte, tj.:

1. W Spółce na podstawie uchwały nr […] Zarządu Spółki z dnia […] maja 2014 r. powołany został administrator bezpieczeństwa informacji.
2. Opracowano ewidencję osób upoważnionych do przetwarzania danych osobowych.
3. Uzupełniono dokument o nazwie „Polityka bezpieczeństwa danych osobowych" o wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe; wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych; opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi; sposób przepływu danych pomiędzy poszczególnymi systemami.
4. Sporządzono wzór rejestru naruszeń danych osobowych.

Stosownie do art. 105 § 1 Kodeksu postępowania administracyjnego, gdy postępowanie z jakiejkolwiek przyczyny stało się bezprzedmiotowe w całości albo w części, organ administracji publicznej wydaje decyzję o umorzeniu postępowania odpowiednio w całości albo w części. Przesłanką umorzenia postępowania, na podstawie art. 105 § 1 k.p.a., jest bezprzedmiotowość postępowania „z jakiejkolwiek przyczyny", czyli z każdej przyczyny powodującej brak jednego z elementów materialnoprawnego stosunku prawnego w odniesieniu do jego strony podmiotowej lub przedmiotowej (wyrok NSA z dnia 21 stycznia 1999 r., SA/Sz1029/97).

W toku postępowania usunięte zostały pozostałe uchybienia w procesie przetwarzania danych osobowych, stanowiące przedmiot postępowania i dlatego w tym zakresie należało je 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.

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.).