GENERALNY INSPEKTOR OCHRONY DANYCH OSOBOWYCH

dr Wojciech R. Wiewiórowski

Warszawa, dnia 17 lipca 2014 r.

DIS/DEC-677/14/55366

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. 31 ust. 1 i 2, art. 36 ust. 3, art. 37 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.), § 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 H. S.A.,

I. Nakazuję H. S.A. usunięcie uchybień w procesie przetwarzania danych osobowych poprzez:

1. Zaprzestanie udostępniania przedsiębiorcom, z którymi zawarte zostały umowy o świadczenie usług zarządzania siecią teleinformatyczną, danych osobowych abonentów bez podstawy prawnej, tj. bez zawarcia z ww. przedsiębiorcami umowy powierzenia przetwarzania danych osobowych, o której mowa w art. 31 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.), określającej cel i zakres, w jakim wskazani przedsiębiorcy mogą przetwarzać powierzone im dane osobowe, w terminie 30 dni od dnia, w którym niniejsza decyzja stanie się ostateczna.

2. **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 H. 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 Wiceprezesa Zarządu Spółki oraz prokurenta 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. Niezawarciu w umowach o świadczenie usług zarządzania siecią teleinformatyczną, podpisanych z przedsiębiorcami wykonującymi czynności zarządzania siecią teleinformatyczną,

postanowień określających cel i zakres, w jakim podmioty te mogą przetwarzać powierzone im dane osobowe (art. 31 ust. 2 ustawy).

2. Niezawarciu z M. S.A. umowy powierzenia przetwarzania danych osobowych abonentów Spółki (art. 31 ust. 1 ustawy).
3. Niewyznaczeniu administratora bezpieczeństwa informacji (36 ust. 3 ustawy).
4. Nienadaniu osobom dopuszczonym w Spółce do przetwarzania danych osobowych upoważnień do ich przetwarzania (art. 37 ustawy).
5. Nieprowadzeniu ewidencji osób upoważnionych do przetwarzania danych osobowych (art. 39 ust. 1 ustawy).
6. Niezapewnianiu przez system informatyczny o nazwie „[…]", wykorzystywany do przetwarzania danych osobowych abonentów Spółki, sporządzenia i wydrukowania raportu zawierającego w powszechnie zrozumiałej formie informacje, o których mowa w § 7 ust. 1 rozporządzenia (§ 7 ust. 3 rozporządzenia).
7. 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 […] maja 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. W dniu […] maja 2014 r. została zawarta z M. S.A. umowa powierzenia przetwarzania danych osobowych.
3. Do umów z podmiotami świadczącymi usługi zarządzania siecią teleinformatyczną Spółki sporządzono aneksy zawierające postanowienia określające cel i zakres, w jakim podmioty te mogą przetwarzać dane osobowe.
4. Sporządzono ewidencję osób upoważnionych do przetwarzania danych osobowych, a osobom dopuszczonym do przetwarzania danych nadano upoważnienia do ich przetwarzania.
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 art. 31 ust. 1 ustawy, administrator danych może powierzyć innemu podmiotowi, w drodze umowy zawartej na piśmie, przetwarzanie danych. W myśl art. 31 ust. 2 ustawy, podmiot, o którym mowa w ust. 1, może przetwarzać dane wyłącznie w zakresie i celu przewidzianym w umowie.

W toku kontroli ustalono, że czynności zarządzania siecią teleinformatyczną są wykonywane przez przedsiębiorców, z którymi Spółka zawarła umowy o świadczenie usług zarządzanie siecią teleinformatyczną. Przedsiębiorcy świadczący na rzecz Spółki usługi w zakresie zarządzania siecią teleinformatyczną posiadają dostęp do danych osobowych abonentów Spółki. W podpisanych umowach z tymi podmiotami nie zostały jednak zawarte postanowienia określające cel i zakres, w jakim podmioty te mogą przetwarzać powierzone im dane osobowe.

W odpowiedzi na zawiadomienie o wszczęciu postępowania administracyjnego wyznaczony w Spółce administrator bezpieczeństwa informacji pismem z dnia […] maja 2014 r., nr […], poinformował, że do umów z ww. podmiotami sporządzono aneksy zawierające postanowienia określające cel i zakres, w jakim podmioty te mogą przetwarzać dane osobowe. Do wskazanego pisma, jak również do pisma z dnia […] czerwca 2014 r., nr […], nie została jednak dołączona kserokopia przykładowego aneksu, pomimo wezwania Spółki do przedstawienia takiego aneksu przez Generalnego Inspektora w piśmie z dnia […] czerwca 2014 r., nr […]. Co więcej, w piśmie z dnia […] czerwca 2014 r., nr […], wyznaczony w Spółce administrator bezpieczeństwa informacji poinformował o przygotowaniu aneksu do umowy zawartej z A. Sp. z o.o., gdy tymczasem przedmiotem postępowania objęty jest brak postanowień określających cel i zakres, w jakim mogą przetwarzać powierzone im dane osobowe podmioty, z którymi Spółka podpisała umowy o świadczenie usług zarządzanie siecią teleinformatyczną, tj. podmioty wymienione na wykazie stanowiącym załącznik nr […] do protokołu kontroli. Wśród podmiotów wymienionych na tym wykazie nie figuruje A. Sp. z o.o.

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 nie

ustosunkował się do ww. uchybienia w procesie przetwarzania danych osobowych, ani też nie przedstawił żadnych dowodów, z których wynikałoby, że w tym zakresie Spółka przywróciła stan zgodny z prawem.

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. W dniu […] maja 2014 r. została zawarta z M. S.A. umowa powierzenia przetwarzania danych osobowych, określająca zakres i cel, w jakim wskazany podmiot może przetwarzać powierzone mu dane osobowe abonentów Spółki.
3. Osobom dopuszczonym do przetwarzania danych osobowych nadano upoważnienia do ich przetwarzania.
4. Opracowano ewidencję osób upoważnionych do przetwarzania danych osobowych.
5. 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.).