GENERALNY INSPEKTOR OCHRONY DANYCH OSOBOWYCH
dr Wojciech R. Wiewiórowski

Warszawa, dnia 5 lipca 2013 r.

DIS/DEC-722/13/42803
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 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. 7 pkt 5, art. 23 ust. 1 pkt 1 i art. 36 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.) w sprawie przetwarzania danych osobowych przez S. Sp. z o.o.,

1. Nakazuję S Sp. z o.o., usunięcie uchybień w procesie przetwarzania danych, poprzez zastosowanie środków kryptograficznej ochrony wobec danych wykorzystywanych do uwierzytelnienia w systemie informatycznym o nazwie „A." oraz wobec danych osobowych wprowadzanych na stronie www. w procesie rejestracji konta w systemie informatycznym o nazwie „A", w terminie do dnia [...]
2. 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 w S. Sp. z o.o., dalej zwaną „Spółką", kontrolę 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".

Zakresem kontroli objęto przetwarzanie przez S. Sp. z o.o. danych osobowych w związku z prowadzonymi programami lojalnościowymi oraz w związku z wykorzystaniem technologii identyfikacji radiowej - RFID (ang. Radio Frequency Identification). W toku kontroli odebrano ustne wyjaśnienia od pracowników Spółki oraz skontrolowano systemy informatyczne służące do przetwarzania danych osobowych. Stan faktyczny został szczegółowo opisany w protokole kontroli, który został podpisany przez pełnomocnika Spółki (pełnomocnictwo z dnia [...]).

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. Braku możliwości wyrażenia w sposób swobodny przez klientów przystępujących do programu lojalnościowego o nazwie [...] oświadczenia woli, którego treścią jest zgoda na przetwarzanie danych osobowych, odrębnie w celu realizacji ww. programu, odrębnie na każdy z pozostałych wymienionych celów przetwarzania danych (tj. w celach marketingowych i handlowych oraz w celu ochrony praw podmiotów należących do [...], a w szczególności [...] i wszystkich jej oddziałów, w celu przekazywania podmiotom należącym do [...], w tym [...] ich filiom, oddziałom, ich usługodawcom) (art. 23 ust. 1 pkt 1 w zw. z art. 7 pkt 5 ustawy).

2. Przesyłaniu danych osobowych wprowadzanych w formularzu na stronie www, w procesie rejestracji konta w systemie informatycznym o nazwie „A" (służącym do przetwarzania danych osobowych klientów Spółki) w postaci niezapewniającej ochrony odpowiedniej do zagrożeń tj. poprzez nieszyfrowaną stronę www (art. 36 ust. 1 ustawy).

3. Niezastosowaniu wymaganych środków kryptograficznej ochrony wobec danych wykorzystywanych do uwierzytelnienia, które są przesyłane w sieci publicznej w trakcie procesu logowania w systemie informatycznym o nazwie „A" (służącym do przetwarzania danych osobowych klientów Spółki) (art. 36 ust. 1 ustawy).

W związku z powyższym, w dniu [...] maja 2013 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, pełnomocnicy Spółki pismami z dnia [...] czerwca 2013 r. oraz [...] czerwca 2013 r. i [...] czerwca 2013 r. złożyli wyjaśnienia, z których wynika, że:

1. Zmieniony został formularz dla klientów przystępujących do programu lojalnościowego o nazwie [...], w ten sposób, że w oświadczeniu o wyrażeniu zgody na przetwarzanie danych zostały na nowo określone cele, w którym przetwarzane są dane osobowe osoby składającej to oświadczenie, jako cele związane z uczestnictwem w Programie [...], a w szczególności promowania produktów i usług S.

2. Rozpoczęto prace nad zaszyfrowaniem strony www służącej do rejestrowania i logowania się do konta w systemie informatycznym o nazwie „A". Wyjaśniono również, że strona [...], w tym cześć poświęcona [...] jest zarządzana przez [...] (właściciela Spółki) i projekt zaszyfrowania tej strony będzie obejmował wszystkie podmioty wchodzące w skład tego podmiotu. Przedstawiono również harmonogram prac w ramach ww. projektu i określono termin wdrożenia zmian na [...]

Generalny Inspektor Ochrony Danych Osobowych po przeprowadzeniu analizy całokształtu materiału dowodowego zebranego w niniejszej sprawie 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.

W toku czynności kontrolnych ustalono, że proces rejestracji konta w systemie informatycznym o nazwie „A" (służącym do przetwarzania danych osobowych klientów Spółki) odbywa się poprzez nieszyfrowaną stronę www. Tym samym należy uznać, że dane osobowe wprowadzane w formularzu na stronie www przesyłane są w postaci niezapewniającej ochrony odpowiedniej do zagrożeń. Ponadto ustalono, że proces logowania w systemie informatycznym o nazwie „A." (służącym do przetwarzania danych osobowych klientów Spółki) odbywa się poprzez nieszyfrowaną stronę www. Administrator danych nie zastosował zatem wymaganych środków kryptograficznej ochrony wobec danych wykorzystywanych do uwierzytelnienia, które są przesyłane w sieci publicznej.

Biorą pod uwagę wyjaśnienia pełnomocników Spółki dotyczące podjęcia działań nad zaszyfrowaniem strony www. służącej do rejestrowania i logowania się do konta w systemie

informatycznym o nazwie „A.”, należy uznać, że nie są one wystarczające do uznania, iż wskazane uchybienia zostały usunięte. Generalny Inspektor Ochrony Danych Osobowych nakazuje zatem przywrócenie stanu zgodnego z prawem w zakresie powyższych uchybień, uwzględniając jednak wskazany przez Spółkę termin.

Na podstawie przedstawionych dowodów należy natomiast stwierdzić, że pozostałe uchybienia w procesie przetwarzania danych osobowych, stanowiące przedmiot postępowania, zostały usunięte, tj. zapewniona została swoboda klientom przystępującym do programu lojalnościowego o nazwie [...], składającym oświadczenie woli, którego treścią jest zgoda na przetwarzanie danych osobowych w zakresie wyboru celów przetwarzania tych danych.

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 21 stycznia 1999 r. S.A./Sz1029/97).

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.).