GENERALNY INSPEKTOR
OCHRONY DANYCH
OSOBOWYCH
dr Wojciech R. Wiewiórowski

Warszawa, dnia 14 czerwca 2013 r.

DIS/DEC-628/13/37521
dot. [...]

D E C Y Z J A

Na podstawie 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. 38, 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.), § 4 pkt 1 i pkt 3, § 7 ust.1 pkt 1 i pkt 2, § 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), częścią A pkt II ust. 2 lit. b i pkt IV ust. 2 załącznika do ww. rozporządzenia, po przeprowadzeniu postępowania w sprawie przetwarzania danych osobowych przez A Sp. z o. o.,

umarzam postępowanie w niniejszej sprawie

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

Inspektorzy upoważnieni przez Generalnego Inspektora Ochrony Danych Osobowych przeprowadzili kontrolę (sygn. akt [...]) w A Sp. z o. o., dalej zwanej również „Spółką”, w celu ustalenia zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych, 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 danych osobowych przez A. Sp. z o. o., w związku z prowadzonymi programami lojalnościowymi oraz w związku z wykorzystaniem technologii identyfikacji radiowej - RFID (ang. Radio Frequency Identification). W toku kontroli odebrano od pracowników Spółki ustne wyjaśnienia oraz skontrolowano systemy informatyczne, w których przetwarzane są dane osobowe. Stan faktyczny został szczegółowo opisany w protokole kontroli, który został podpisany przez członka Zarządu Spółki.

Na podstawie tak zgromadzonego materiału dowodowego ustalono, że w procesie przetwarzania danych osobowych Spółka jako administrator danych, naruszyła przepisy o ochronie danych osobowych. Postępowaniem administracyjnym wszczętym w dniu [...] marca 2013 r. (sygn. pisma [...]) objęto:

1. Niezastosowanie mechanizmów kontroli dostępu do danych przetwarzanych w systemie „A.”, polegające na braku dla każdego operatora loginu i hasła przy logowaniu do rejestratorów tego systemu (część A pkt II ust. 2 lit. b załącznika do rozporządzenia).
2. Niedopełnienie obowiązku zmiany, nie rzadziej niż co 30 dni, hasła do systemu informatycznego „B.” (w którym przetwarzane są dane osobowe pracowników Spółki) (część A pkt IV ust. 2 załącznika do rozporządzenia).
3. Nieuwzględnienie w opracowanej i wdrożonej w Spółce dokumentacji przetwarzania danych osobowych stanowiącej politykę bezpieczeństwa [...] wykazu budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe na serwerze centralnym systemu „C.” (w którym przetwarzane są dane osobowe klientów Spółki) oraz opisu struktury zbiorów danych wskazującego zawartość poszczególnych pól informacyjnych i powiązania między nimi, zawierającego informacje o wizerunku klientów, przetwarzane w systemie monitoringu wizyjnego Spółki (§ 4 pkt 1 i pkt 3 rozporządzenia).
4. Niezapewnienie, aby system informatyczny o nazwie „B.” (w którym przetwarzane są dane osobowe pracowników Spółki) umożliwiał odnotowanie daty pierwszego wprowadzenia danych osobowych do systemu oraz identyfikatora użytkownika wprowadzającego dane do systemu (art. 38 ustawy w zw. z § 7 ust.1 pkt 1 i pkt 2 rozporządzenie).
5. Niezapewnienie, aby system informatyczny o nazwie „C”. (w którym przetwarzane są dane osobowe pracowników Spółki) umożliwiał sporządzenie i wydrukowanie raportu zawierającego w powszechnie zrozumiałej formie informacje, o których mowa w § 7 ust. 1 pkt 1 i pkt 2 rozporządzenia (art. 38 ustawy w zw. § 7 ust. 3 rozporządzenia).

6. Niedopełnienie obowiązku zgłoszenia Generalnemu Inspektorowi zmiany informacji w zbiorze danych uczestników programu o nazwie [...], tj. zbiorze danych o nazwie „M.” (zgłoszenie nr: R [...]) w zakresie podstawy prawnej przetwarzania danych, płci osoby korzystającej z karty [...], płci i daty urodzenia dzieci, nr karty, kodu kreskowego, [...] (dostępne środki, saldo, przedawnione środki), transakcji (data i czas, nr paragonu, nr kasy, zmiana [...]) oraz nr konta [...] (art. 41 ust. 2 ustawy).

W odpowiedzi na pismo informujące o wszczęciu postępowania administracyjnego prokurent Spółki (prokura samoistna) pismem z dnia [...] kwietnia 2013 r., złożył wyjaśnienia w sprawie wskazanych uchybień informując o następujących okolicznościach:

1. W Spółce wprowadzona została kontrola dostępu do systemu „A.” Operatorzy „A.” uzyskują dostęp do systemu monitoringu wizyjnego poprzez podanie indywidualnego identyfikatora i hasła.
2. Dostęp do systemu informatycznego o nazwie „B.” jest możliwy jedynie po dokonaniu uwierzytelnienia w domenie Windows. Każdy użytkownik posiada indywidualny identyfikator w tej domenie i hasło, którego zmianę system wymusza co 30 dni. Użytkownicy systemu „B.” posiadają również indywidualne identyfikatory i hasła, do których zmiany co 30 dni zostali zobowiązani.
3. Polityka bezpieczeństwa A. Sp. z o. o. została zaktualizowana w zakresie określenia obszaru przetwarzania danych, w którym znajduje się centralny serwer systemu informatycznego o nazwie D. Ponadto, uzupełniono ww. dokument w zakresie opisu struktury zbiorów o informacje o wizerunku (przetwarzane w systemie monitoringu wizyjnego).
4. System informatyczny „B.” w logach systemowych oraz bazie danych przechowuje informacje o dacie pierwszego wprowadzenia danych oraz identyfikatorze użytkownika wprowadzającego dane osobowe do systemu. Na podstawie tych danych administrator systemu przygotowuje raport zawierający wymagane informacje.
5. Przygotowano wniosek aktualizacyjny zbioru danych osobowych o nazwie „M.”.

Na potwierdzenie powyższych wyjaśnień pismem z dnia [...] maja 2013 r. prokurent Spółki przesłał: wydruki zawierające wykazy kont użytkowników systemu „A.”, kopie fragmentów z polityki bezpieczeństwa zawierające zaktualizowane i uzupełnione treści, wydruk z systemu informatycznego „B.” zawierający wymagane odnotowania oraz wniosek aktualizacyjny do zgłoszenia zbioru o nazwie „M.”

Generalny Inspektor Ochrony Danych Osobowych po przeprowadzeniu analizy całokształtu materiału dowodowego zebranego w niniejszej sprawie zważył, co następuje:

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).

Na podstawie całokształtu materiału dowodowego należy uznać, iż w toku postępowania administracyjnego zostały usunięte uchybienia w procesie przetwarzania danych osobowych, stanowiące przedmiot postępowania, bowiem:

1. Zapewniono, aby dostęp do danych przetwarzanych w systemie „A." był możliwy po wprowadzeniu indywidualnego dla każdego operatora loginu i hasła (załączono wydruk z systemu zawierający wykaz kont użytkowników).
2. Wprowadzono obowiązek zmiany co 30 dni hasła do systemu informatycznego o nazwie „B." (w którym przetwarzane są dane osobowe pracowników Spółki).
3. Zaktualizowano opracowaną i wdrożoną w Spółce politykę bezpieczeństwa w zakresie wykazu budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe na serwerze centralnym systemu „C." (w którym przetwarzane są dane osobowe klientów Spółki) oraz uzupełniono ww. dokument w zakresie opisu struktury zbiorów danych wskazującego zawartość poszczególnych pól informacyjnych i powiązania między nimi, zawierającego informacje o wizerunku klientów przetwarzanego przez system monitoringu wizyjnego Spółki (załączono wyciąg z polityki bezpieczeństwa zawierający zaktualizowane treści).
4. Przedstawiono wydruki z logu systemowego systemu „B." (w którym przetwarzane są dane osobowe pracowników Spółki) zawierające informacje dotyczące daty pierwszego wprowadzenia danych osobowych do systemu oraz identyfikatora użytkownika wprowadzającego dane do systemu.
5. Zapewniono możliwość sporządzenia i wydrukowania z systemu informatycznego nazwie „B." (w którym przetwarzane są dane osobowe pracowników) raportu zawierającego w powszechnie zrozumiałej formie informacje dotyczące daty pierwszego wprowadzenia danych osobowych do systemu oraz identyfikatora użytkownika wprowadzającego dane do systemu.
6. Dokonano zgłoszenia zmian w zbiorze danych uczestników programu o nazwie [...], tj. zbiorze danych o nazwie „M." (zgłoszenie nr R: [...]) w zakresie podstawy prawnej przetwarzania danych oraz informacji dotyczących płci osoby korzystającej z karty [...], płci i daty urodzenia dzieci oraz danych karty [...]: nr karty, kodu kreskowego, dostępne środki, saldo, przedawnione środki, transakcji (data i czas, nr paragonu, nr kasy), zmiana karty.

Postępowanie administracyjne należało umorzyć, bowiem stało się bezprzedmiotowe.

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.