GENERALNY INSPEKTOR OCHRONY DANYCH OSOBOWYCH

dr Wojciech R. Wiewiórowski

Warszawa, dnia 7 listopada 2014 r.

DIS/DEC-1077/14/87970

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 z późn. zm.), art. 12 pkt 2, art. 18 ust. 1 pkt 1 i art. 22 w związku z art. 36 ust. 1 i 2 oraz art. 41 ust. 1 pkt 2, 3 i 3a ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2014 r., poz. 1182), § 3 ust. 2 i § 4 pkt 2 i 4 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 częścią A pkt IV ust. 2 zd. 1 i częścią C pkt XIII załącznika do rozporządzenia, po przeprowadzeniu postępowania administracyjnego w sprawie przetwarzania danych osobowych przez K. Sp. z o.o.,

I. **Nakazuję K. Sp. z o.o. usunięcie uchybień w procesie przetwarzania danych osobowych, poprzez uzupełnienie dokumentu o nazwie „[…]" o opis przepływu danych pomiędzy poszczególnymi systemami oraz wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych, uwzględniające system informatyczny o nazwie „[…]" (wykorzystywany do przetwarzania danych osobowych osób, które założyły konto w ww. systemie), w terminie 30 dni 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 K. Sp. z o.o., 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 2014 r., poz. 1182), 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 Spółkę danych osobowych osób w związku z rezerwacją i zakupem biletów na przejazd (przewóz). 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 Prezesa Zarządu i Wiceprezesa Zarządu.

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. Umożliwieniu dostępu do modułu administracyjnego systemu „[…]" o nazwie „[…]" bez odpowiednich zabezpieczeń, tj. zastosowanie protokołu http (art. 36 ust. 1 ustawy).
2. Nieuwzględnieniu systemu „[…]" w opisie przepływu danych pomiędzy poszczególnymi systemami oraz w wykazie zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych (§ 3 ust. 2 oraz § 4 pkt 2 i 4 rozporządzenia).
3. Niewskazaniu w zgłoszeniu do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych zbioru danych osobowych o nazwie „[…]" zgody na przetwarzanie danych osobowych jako podstawy prawnej upoważniającej administratora danych do prowadzenia zbioru danych oraz niepodaniu pełnego zakresu danych przetwarzanych w ramach ww. zbioru oraz wszystkich celów przetwarzania tych danych (art. 41 ust. 1 pkt 2, 3 i 3a ustawy).
4. Niezmienianiu przez użytkowników haseł dostępu do systemu „[…]" moduł „[…]" (część A pkt IV ust. 2 zd. 1 załącznika do rozporządzenia).

W związku z powyższym, w dniu […] października 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 Prezes Zarządu oraz Wiceprezes Zarządu pismem z dnia […] października 2014 r., […], złożyli wyjaśnienia, w których poinformowali, że:

1. Stosowanie protokołu https jest obecnie wymuszane automatycznie. Użytkowany jest certyfikat wystawiony przez P. Sp. z o.o.
2. Dokument o nazwie „[…]" zostanie uzupełniony o opis systemu „[…]" niezwłocznie po otrzymaniu stosownej dokumentacji z P. Sp. z o.o.
3. Spółka dokonała zmian w zgłoszeniu do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych zbioru danych osobowych o nazwie „[…]" w zakresie podstawy prawnej przetwarzania danych osobowych, celu przetwarzania oraz zakresu danych przetwarzanych w zbiorze danych.
4. Do czasu wdrożenia funkcjonalności polegającej na wymuszeniu zmiany haseł nie rzadziej niż co 30 dni wprowadzone zostało rozwiązanie doraźne. Użytkownicy są wzywani przez administratora do zmiany hasła.

Ponadto, do pisma z dnia […] października 2014 r., […], Prezes Zarządu oraz Wiceprezes Zarządu przedstawili 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. 36 ust. 2 ustawy, administrator danych prowadzi dokumentację opisującą sposób przetwarzania danych oraz środki, o których mowa w ust. 1. Stosownie do § 3 ust. 2 rozporządzenia, administrator danych prowadzi dokumentację opisującą sposób przetwarzania danych oraz środki, o których mowa w ust. 1. W myśl § 4 pkt 2 i 4 rozporządzenia, polityka bezpieczeństwa, o której mowa w § 3 ust. 1, zawiera w szczególności wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych oraz sposób przepływu danych pomiędzy poszczególnymi systemami.

W toku kontroli ustalono, że w Spółce został opracowany dokument o nazwie „[…]". W ww. dokumencie, w opisie przepływu danych pomiędzy poszczególnymi systemami oraz w wykazie zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych, nie został jednak uwzględniony system „[…]" (wykorzystywany do przetwarzania danych osobowych osób, które założyły konto w ww. systemie).

W odpowiedzi na zawiadomienie o wszczęciu postępowania administracyjnego Prezes Zarządu oraz Wiceprezes Zarządu wskazali, że dokument o nazwie „[…]" zostanie uzupełniony o opis odnoszący się do systemu „[…]" niezwłocznie po otrzymaniu stosownej dokumentacji z P.

Sp. z o.o. Podjęcie tych działań nie może jednak stanowić podstawy do uznania, że w ww. zakresie przywrócony został stan zgodny z prawem. Wskazany dokument nadal bowiem nie zawiera elementów określonych w § 4 pkt 2 i 4 rozporządzenia w odniesieniu do systemu „[…]".

Jednocześnie, na podstawie złożonych przez Prezesa Zarządu oraz Wiceprezesa Zarządu pisemnych wyjaśnień oraz przedstawionych dowodów, należy stwierdzić, że pozostałe uchybienia w procesie przetwarzania danych osobowych, stanowiące przedmiot postępowania, zostały usunięte, tj.:

1. Dostęp do modułu administracyjnego systemu „[…]" o nazwie „[…]" jest możliwy wyłącznie przy wykorzystaniu protokołu https.
2. Dokonano zmian w zgłoszeniu do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych zbioru danych osobowych o nazwie „[…]" w zakresie podstawy prawnej przetwarzania danych osobowych, celu przetwarzania oraz zakresu danych przetwarzanych w zbiorze danych.
3. Hasła do systemu „[…]" są zmieniane co 30 dni.

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 materialnego 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 2012 r., poz. 1015 z późn. zm.).