GENERALNY INSPEKTOR OCHRONY DANYCH OSOBOWYCH

dr Wojciech R. Wiewiórowski

Warszawa, dnia 18 czerwca 2014 r.

DIS/DEC-577/14/47158

dot. […]

D E C Y Z J A

Na podstawie art. 104 § 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. 2 i 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.) oraz § 3 ust. 1 i § 4 pkt 1 – 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), po przeprowadzeniu postępowania administracyjnego w sprawie przetwarzania przez N. Sp. z o.o.,

Nakazuję N. Sp. z o.o. usunięcie uchybień w procesie przetwarzania danych osobowych, poprzez:

1. **Wyznaczenie administratora bezpieczeństwa informacji, w terminie 7 dni od dnia, w którym niniejsza decyzja stanie się ostateczna.**
2. **Nadanie upoważnień do przetwarzania danych osobowych pracownikom N. Sp. z o.o. dopuszczonym do przetwarzania tych danych, w terminie 7 dni od dnia, w którym niniejsza decyzja stanie się ostateczna.**
3. **Opracowanie ewidencji osób upoważnionych do przetwarzania danych osobowych, w terminie 7 dni od dnia, w którym niniejsza decyzja stanie się ostateczna.**

4. **Opracowanie i wdrożenie instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, w terminie 30 dni od dnia, w którym niniejsza decyzja stanie się ostateczna.**
5. **Uzupełnienie dokumentu 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 oraz sposób przepływu danych pomiędzy poszczególnymi systemami, w terminie 30 dni od dnia, w którym niniejsza decyzja stanie się ostateczna.**

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

Inspektorzy upoważnieni przez Generalnego Inspektora Ochrony Danych Osobowych, przeprowadzili w N. Sp. z o.o., zwanej dalej Spółką, kontrolę zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych (sygn. […]), 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, i 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 abonentów H. S.A., H. Sp. z o.o., M. S.A. i P. S.A. w związku z administrowaniem systemem informatycznym służącym do obsługi platformy […], wykorzystywanej do przetwarzania danych abonentów ww. podmiotów. W toku kontroli odebrano od pracowników Spółki ustne wyjaśnienia oraz skontrolowano systemy informatyczne wykorzystywane do przetwarzania 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 (art. 36 ust. 3 ustawy).
2. Nienadaniu osobom dopuszczonym w Spółce do przetwarzania danych osobowych upoważnień do ich przetwarzania (art. 37 ustawy).

3. Braku ewidencji osób upoważnionych do przetwarzania danych osobowych (art. 39 ust. 1 ustawy).
4. Nieopracowaniu dokumentacji stanowiącej instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych (art. 36 ust. 2 ustawy i § 3 ust. 1 rozporządzenia).
5. Niezawarciu w 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 wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi oraz sposobu przepływu danych pomiędzy poszczególnymi systemami (§ 4 pkt 1 – 4 rozporządzenia).

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 […]).

Spółka nie ustosunkowała się pisemnie do stwierdzonych uchybień w procesie przetwarzania danych osobowych, stanowiących przedmiot postępowania administracyjnego, wymienionych w zawiadomieniu o wszczęciu postępowania.

Po zapoznaniu się z całością materiału dowodowego zebranego w sprawie Generalny Inspektor Ochrony Danych Osobowych zważył co następuje:

Zgodnie z art. 36 ust. 3 ustawy, administrator danych wyznacza administratora bezpieczeństwa informacji, nadzorującego przestrzeganie zasad ochrony, o których mowa w ust. 1, chyba że sam wykonuje te czynności.

Przeprowadzona kontrola wykazała, że w Spółce nie został wyznaczony administrator bezpieczeństwa informacji, co stanowi naruszenie ww. przepisu ustawy.

Zgodnie z art. 37 ustawy, do przetwarzania danych mogą być dopuszczone wyłącznie osoby posiadające upoważnienie nadane przez administratora danych.

W toku kontroli ustalono, iż osobom dopuszczonym w Spółce do przetwarzania danych osobowych nie zostały nadane upoważnienia do ich przetwarzania, co stanowi naruszenie powołanego przepisu ustawy.

Zgodnie z art. 39 ust. 1 ustawy, administrator danych prowadzi ewidencję osób upoważnionych do ich przetwarzania, która powinna zawierać: 1) imię i nazwisko osoby upoważnionej, 2) datę nadania i ustania oraz zakres upoważnienia do przetwarzania danych osobowych, 3) identyfikator, jeżeli dane są przetwarzane w systemie informatycznym.

W toku kontroli ustalono, że w Spółce nie jest prowadzona ewidencja osób upoważnionych do przetwarzania danych osobowych, co stanowi naruszenie ww. przepisu ustawy.

Zgodnie z art. 36 ust. 2 ustawy, administrator danych prowadzi dokumentację opisującą sposób przetwarzania danych oraz środki, o których mowa w ust. 1. W myśl § 3 ust. 1 rozporządzenia, na dokumentację, o której mowa w § 1 pkt 1, składa się polityka bezpieczeństwa i instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, zwana dalej „instrukcją".

Przeprowadzona kontrola wykazała, że w Spółce nie została opracowana dokumentacja stanowiąca instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, co stanowi naruszenie ww. przepisów ustawy i rozporządzenia.

Zgodnie z § 4 pkt 1 – 4 rozporządzenia, polityka bezpieczeństwa, o której mowa w § 3 ust. 1, zawiera w szczególności 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 oraz sposób przepływu danych pomiędzy poszczególnymi systemami.

Obowiązujący w Spółce dokument o nazwie „Polityka bezpieczeństwa danych osobowych" nie zawiera 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 wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi oraz sposobu przepływu danych pomiędzy poszczególnymi systemami, tj. elementów wymaganych przez ww. przepis rozporządzenia

Wobec powyższego, Generalny Inspektor Ochrony Danych Osobowych rozstrzygnął jak w sentencji.

Na podstawie art. 21 ust. 1 ustawy o ochronie danych osobowych i 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.).