GENERALNY INSPEKTOR
OCHRONY DANYCH
OSOBOWYCH
dr Wojciech R. Wiewiórowski

Warszawa, dnia 25 lipca 2014 r.

DIS/DEC-707/57900/14
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 art. 31 ust. 1 i 2, art. 36 ust. 2 i 3 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 4, § 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. Sp. z o.o.;

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

1. Zaprzestanie powierzania przetwarzania danych [...] przedsiębiorcom, z którymi H. Sp. z o.o. zawarła umowy o świadczenie usług [...], bez zawarcia z nimi pisemnych umów powierzenia przetwarzania ww. danych osobowych zgodnie z art. 31 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.), określających 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. Zapewnienie, aby system informatyczny o nazwie A (wykorzystywany do przetwarzania danych osobowych [...]) umożliwiał 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.

Uzasadnienie

Inspektorzy upoważnieni przez Generalnego Inspektora Ochrony Danych Osobowych przeprowadzili kontrolę w H. Sp. z o.o. (zwanej dalej również „Spółką"), w celu ustalenia zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych (sygn. kontroli [...]), 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". W toku kontroli odebrano od pracowników Spółki ustne wyjaśnienia, oraz skontrolowano systemy informatyczne w których odbywa się przetwarzanie danych osobowych. Stan faktyczny został szczegółowo opisany w protokole kontroli, który został podpisany przez prokurenta oraz 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. Niezawarciu z przedsiębiorcami, z którymi Spółka podpisała umowy o świadczenie usług [...] (posiadającymi dostęp do danych [...]), pisemnych umów powierzenia przetwarzania danych osobowych [...] (art. 31 ust. 1 i 2 ustawy).

2. Niezawarciu z M. S.A. pisemnej umowy powierzenia przetwarzania danych osobowych [...] (art. 31 ust. 1 i 2 ustawy).

3. Nieprowadzeniu rejestru naruszeń danych osobowych, o którym mowa w art. 174d ust. 1 ustawy z dnia 16 lipca 2004 r. Prawo telekomunikacyjne (Dz. U. Nr 171, poz. 1800 z późn. zm.).

4. Niezapewnieniu, aby dokumentacja opisująca sposób przetwarzania danych osobowych w Spółce oraz środki techniczne i organizacyjne zapewniające ich ochronę spełniła wymogi, o których mowa w § 4 pkt 1 i pkt 4 rozporządzenia.

5. Niezapewnieniu, aby system informatyczny o nazwie A (wykorzystywany do przetwarzania danych osobowych [...]) umożliwiał sporządzenie i wydrukowanie raportu zgodnie § 7 ust. 3 rozporządzenia.

6. Niepowołaniu administratora bezpieczeństwa informacji nadzorującego przestrzeganie zasad ochrony, o których mowa w art. 36 ust. 1 ustawy o ochronie danych osobowych (art. 36 ust. 3 ustawy).

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. Pismem zawiadamiającym o wszczęciu postępowania administracyjnego w przedmiotowej sprawie (znak: [...]) administrator danych został poinformowany o prawie czynnego udziału w każdym stadium postępowania, a przed wydaniem decyzji wypowiedzenia się co do zebranych dowodów i materiałów oraz zgłoszonych żądań.

W odpowiedzi na zawiadomienie o wszczęciu postępowania administracyjnego Spółka pismem z dnia [...] czerwca 2014 r. złożyła wyjaśnienia w zakresie stwierdzonych uchybień oraz dowody mające potwierdzić ich usunięcie. Z udzielonych wyjaśnień wynika, że:

1. Z dniem [...] maja 2014 r. powołano administratora bezpieczeństwa informacji dla H. Sp. z o.o.

2. Z uwagi na to, iż obecnie Spółka nie zatrudnia pracowników upoważnionych do przetwarzania danych osobowych, z dniem [...] czerwca 2014 r. została zawarta z M. S.A. umowa powierzenia przetwarzania danych osobowych [...].

3. Trwa proces negocjacji umów z administratorami sieci Spółki. Do umów z ww. podmiotami [...] sporządzono aneksy dotyczące postanowień określających cel i zakres, w jakim podmioty te mogą przetwarzać dane osobowe.

4. Sporządzono wzór rejestru naruszeń danych osobowych, o którym mowa w art. 174d ust. 1 ustawy z dnia 16 lipca 2004 r. Prawo telekomunikacyjne (Dz. U. Nr 171, poz. 1800 z późn. zm.).

5. Uzupełniono „Politykę bezpieczeństwa [...]" o załączniki zawierające wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych oraz informacje o sposobie przepływu danych pomiędzy poszczególnymi systemami.

Do wskazanych wyjaśnień załączono następujące dowody: kopię uchwały nr [...] Zarządu Spółki z dnia [...] maja 2014 r. w sprawie powołania administratora bezpieczeństwa informacji; kopię umowy powierzenia przetwarzania danych osobowych z dnia [...] czerwca 2014 r. zawartej przez Spółkę z M. S.A.; wzór prowadzonego w Spółce rejestru naruszeń danych osobowych; załączniki do „Polityki bezpieczeństwa [...]" zawierające: „Wykaz budynków i pomieszczeń w Spółce, tworzących obszary, w których przetwarzane są dane osobowe" (załącznik nr [...]), „Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych" (załącznik nr [...]), „Opis struktur zbiorów danych" (załącznik nr [...]), „Sposób przepływu danych pomiędzy poszczególnymi systemami" (załącznik nr [...]), „Środki

techniczne i organizacyjne zabezpieczające dane osobowe" (załącznik nr [...]). Nie załączono natomiast kopii aneksów do zawartych umów o świadczenie usług [...]. Jednocześnie Spółka zwróciła się o przedłużenie terminu na ich przekazanie do dnia [...] lipca 2014 r.

Po zapoznaniu się z całością materiału dowodowego zebranego w niniejszej 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 podmioty, z którymi Spółka zawarła umowy o świadczenie usług [...], tj. przedsiębiorców, którzy posiadają dostęp do wszystkich danych aktualnych klientów Spółki korzystających z dostępu do internetu w technologii [...]. W powołanych umowach o świadczenie usług [...] zawartych z ww. przedsiębiorcami, nie zostały jednak zamieszczone postanowienia określające cel i zakres, w jakim mogą przetwarzać powierzone im dane osobowe.

Jak wynika z wyjaśnień Spółki, aktualnie trwa proces negocjacji umów [...]. Sporządzono już stosowne aneksy do ww. umów, które regulują kwestie związane z powierzeniem im przez Spółkę przetwarzania danych osobowych. Spółka nie przekazała kopii podpisanych aneksów z powodu – jak wyjaśniono – występujących w nich braków formalnych.

Odnosząc się do powyższych wyjaśnień należy wskazać, iż samo podjęcie działań, które mają na celu zapewnienie, iż dane osobowe [...] będą przetwarzanie przez Spółkę zgodnie z art. 31 ust. 1 i 2 ustawy, nie może stanowić podstawy dla uznania, iż w przedmiotowym zakresie został przywrócony stan zgodny z prawem. Generalny Inspektor formułując nakaz niniejszej decyzji uwzględnił jednak działania podjęte przez Spółkę i wyznaczył termin usunięcia ww. uchybienia zgodny ze złożonym przez Spółkę wnioskiem.

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 § 7 ust. 1 rozporządzenia.

W toku czynności kontrolnych ustalono, że system informatyczny wykorzystywany do przetwarzania danych osobowych [...] zwany A zapewnia automatyczne odnotowanie daty i identyfikatora użytkownika wprowadzającego dane. System A nie umożliwia jednak sporządzenia i wydrukowania raportu zawierającego w powszechnie zrozumiałej formie ww. informacje. Tym samym ww. system nie spełnia wymogów wynikających z § 7 ust. 3 rozporządzenia.

W piśmie stanowiącym odpowiedź na zawiadomienie o wszczęciu postępowania administracyjnego nie ustosunkowano się do ww. uchybienia w procesie przetwarzania danych osobowych, ani nie przedstawiono dowodów potwierdzających jego usunięcie.

Jednocześnie, na podstawie złożonych pismem z dnia [...] czerwca 2014 r. wyjaśnień oraz załączonych do niego innych dowodów, należy stwierdzić, że pozostałe uchybienia w procesie przetwarzania danych osobowych, stanowiące przedmiot postępowania, zostały usunięte, tj.:

1. W dniu [...] czerwca 2014 r. Spółka zawarła z M. S.A. (poprzednia nazwa: M. S.A.) umowę powierzenia przetwarzania danych osobowych, która określa zakres i cel w jakim ww. podmiot może przetwarzać powierzone mu dane osobowe [...].
2. Sporządzono wzór rejestru naruszeń danych osobowych.
3. Uzupełniono dokumentację opisującą sposób przetwarzania danych osobowych w Spółce oraz środki techniczne i organizacyjne zapewniające ich ochronę o elementy, o których mowa w § 4 pkt 1 i pkt 4 rozporządzenia, tj. wykaz zbiorów danych osobowych wraz ze wskazaniem programów informatycznych zastosowanych do przetwarzania tych danych oraz sposób przepływu danych pomiędzy poszczególnymi systemami.
4. Na podstawie uchwały nr [...] Zarządu Spółki z dnia [...] maja 2014 r. w Spółce powołano administratora bezpieczeństwa informacji.

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).

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.).