GENERALNY INSPEKTOR OCHRONY DANYCH OSOBOWYCH

dr Wojciech R. Wiewiórowski

Warszawa, dnia 13 marca 2014 r.

DIS/DEC-230/14/19293

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. 24 ust. 1, art. 31 ust. 1, art. 36 ust. 1, 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.) oraz częścią C pkt XIII załącznika do 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 danych osobowych przez S. Sp. z o.o.,

Nakazuję S. Sp. z o.o. (zwanej dalej również „Spółką") usunięcie uchybień w procesie przetwarzania danych osobowych poprzez:

1. **Realizowanie wobec osób korzystających z formularza kontaktowego sklepu internetowego [...], osób zakładających konto użytkownika tego sklepu oraz osób dokonujących zakupów w sklepie internetowym [...] bez zakładania konta użytkownika, obowiązku informacyjnego, o którym mowa w art. 24 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 terminie od dnia, w którym niniejsza decyzja stanie się ostateczna.**
2. **Zaprzestanie powierzania danych osób, korzystających z elektronicznego formularza kontaktu sklepu internetowego [...] spółce G. S.A., do czasu zawarcia z ww. podmiotem w przedmiotowym zakresie pisemnej umowy powierzenia przetwarzania danych**

osobowych, o której mowa w art. 31 ust. 1 i 2 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r., Nr 101, poz. 926 z późn. zm.), w terminie od dnia, w którym niniejsza decyzja stanie się ostateczna.

3. **Zaprzestanie powierzania danych osobowych klientów sklepu internetowego [...] zawartych na fakturach VAT, Pani A. F., jako zleceniobiorcy, który zgodnie z zawartą w dniu [...] listopada 2012 r. umową prowadzi księgowość Spółki, do czasu zawarcia z tymże zleceniobiorcą w przedmiotowym zakresie pisemnej umowy powierzenia przetwarzania danych osobowych, o której mowa w art. 31 ust. 1 i 2 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r., Nr 101, poz. 926 z późn. zm.), w terminie od dnia, w którym niniejsza decyzja stanie się ostateczna.**
4. **Zaprzestanie powierzania danych osobowych klientów sklepu internetowego [...] O. Sp. z o.o., do czasu zawarcia z ww. podmiotem w przedmiotowym zakresie pisemnej umowy powierzenia przetwarzania danych osobowych, o której mowa w art. 31 ust. 1 i 2 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r., Nr 101, poz. 926 z późn. zm.), w terminie od dnia, w którym niniejsza decyzja stanie się ostateczna.**
5. **Zaprzestanie powierzania danych osobowych klientów sklepu internetowego [...] Panu G. P., jako zleceniobiorcy, który zgodnie z zawartą w dniu [...] października 2013 r. umową administruje serwerem, na którym znajdują się ww. dane osobowe, do czasu zawarcia z tymże zleceniobiorcą w przedmiotowym zakresie pisemnej umowy powierzenia przetwarzania danych osobowych, o której mowa w art. 31 ust. 1 i 2 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r., Nr 101, poz. 926 z późn. zm.), w terminie od dnia, w którym niniejsza decyzja stanie się ostateczna.**
6. **Zastosowanie środków kryptograficznej ochrony danych wobec danych osobowych przesyłanych w sieci publicznej w związku z procesami tworzenia konta użytkownika na stronie sklepu internetowego [...], logowania się na to konto i tworzenia zamówienia towaru oraz w związku z procesem sprzedaży prowadzonej w sklepie internetowym [...], w terminie 30 dni od dnia, w którym niniejsza decyzja stanie się ostateczna.**
7. **Zgłoszenie Generalnemu Inspektorowi Ochrony Danych Osobowych zmiany informacji zawartych w zgłoszeniu zbioru danych osobowych o nazwie S. (nr [...]) dotyczących: adresu siedziby administratora danych, przedstawiciela Spółki, o którym mowa w art. 31a ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r., Nr 101, poz. 926 z późn. zm.), powierzenia przetwarzania danych osobowych, podstawy prawnej przetwarzania danych osobowych oraz zakresu**

przetwarzanych danych osobowych, 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 kontrolę w S. Sp. z o.o. (zwanej dalej również „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 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 Spółkę danych osobowych, w tym danych osobowych przetwarzanych w zbiorze danych o nazwie S. (zgłoszenie nr [...]) – kontrola z urzędu w związku z pismem Departamentu Rejestracji Zbiorów Danych Osobowych z dnia [...] września 2013 r. [...]. 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 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. Nierealizowaniu wobec osób korzystających z formularza kontaktowego sklepu internetowego [...], osób zakładających konto użytkownika tego sklepu oraz osób dokonujących zakupów w sklepie internetowym [...] bez zakładania konta użytkownika, obowiązku informacyjnego, o którym mowa w art. 24 ust. 1 ustawy.
2. Powierzaniu danych osób, korzystających z elektronicznego formularza kontaktu sklepu internetowego [...] spółce G. S.A., bez pisemnej umowy powierzenia przetwarzania danych osobowych, o której mowa w art. 31 ust. 1 i 2 ustawy.
3. Powierzaniu danych osobowych klientów sklepu internetowego [...] zawartych na fakturach VAT, Pani A. F., bez pisemnej umowy powierzenia przetwarzania danych osobowych, o której mowa w art. 31 ust. 1 i 2 ustawy.

4. Powierzaniu danych osobowych klientów sklepu internetowego [...] spółce O. Sp. z o.o., bez pisemnej umowy powierzenia przetwarzania danych osobowych, o której mowa w art. 31 ust. 1 i 2 ustawy.
5. Powierzaniu danych osobowych klientów sklepu internetowego [...] Panu G. P., bez pisemnej umowy powierzenia przetwarzania danych osobowych, o której mowa w art. 31 ust. 1 i 2 ustawy.
6. Niezastosowaniu odpowiednich środków technicznych i organizacyjnych w celu ochrony danych osobowych przesyłanych w sieci publicznej w związku z procesami tworzenia konta użytkownika na stronie sklepu internetowego [...], logowania się na to konto i tworzenia zamówienia towaru oraz procesem sprzedaży prowadzonej w sklepie internetowym [...] z uwagi na brak środków kryptograficznej ochrony tych danych (art. 36 ust. 1 ustawy w zw. z częścią C pkt VIII rozporządzenia).
7. Niezgłoszeniu Generalnemu Inspektorowi Ochrony Danych Osobowych zmiany informacji zawartych w zgłoszeniu zbioru danych osobowych o nazwie S. (nr [...]) dotyczących: adresu siedziby administratora danych, przedstawiciela Spółki, o którym mowa w art. 31a ustawy, powierzenia przetwarzania danych osobowych, podstawy prawnej przetwarzania danych osobowych oraz zakresu danych osobowych przetwarzanych w tym zbiorze (art. 41 ust. 2 ustawy).

W związku z powyższym, w dniu [...] stycznia 2014 r. Generalny Inspektor Ochrony Danych Osobowych wszczął z urzędu postępowanie administracyjne w niniejszej sprawie w celu wyjaśnienia okoliczności sprawy (sygn. pisma [...]). Spółka, jako administrator danych, została poinformowana o prawie czynnego udziału w każdym stadium postępowania, a przed wydaniem decyzji wypowiedzenia się co do zebranych dowodów i materiałów oraz zgłoszonych żądań. Z powyższego prawa Spółka nie skorzystała.

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

Zgodnie z art. 24 ust. 1 ustawy, w przypadku zbierania danych osobowych od osoby, której one dotyczą, administrator danych jest obowiązany poinformować tę osobę o: 1) adresie swojej siedziby i pełnej nazwie, a w przypadku gdy administratorem danych jest osoba fizyczna – o miejscu swojego zamieszkania oraz imieniu i nazwisku, 2) celu zbierania danych, a w szczególności o znanych mu w czasie udzielania informacji lub przewidywanych odbiorcach lub kategoriach odbiorców danych, 3) prawie dostępu do treści swoich danych oraz ich poprawiania, 4) dobrowolności albo obowiązku podania danych, a jeżeli taki obowiązek istnieje, o jego podstawie prawnej.

Jak ustalono w toku kontroli, Spółka nie udziela osobom, od których pozyskuje dane osobowe, tj. osobom korzystającym z formularza kontaktowego, osobom zakładającym konto użytkownika oraz osobom dokonującym zakupów w sklepie internetowym [...] bez zakładania konta użytkownika, informacji, o których mowa w art. 24 ust. 1 ustawy o ochronie danych osobowych, naruszając w tym zakresie przepisy o ochronie danych osobowych.

Zgodnie z art. 31 ust. 1 ustawy, administrator danych może powierzyć innemu podmiotowi, w drodze umowy zawartej na piśmie, przetwarzanie danych. Stosownie do ust. 2 ww. przepisu, podmiot, o którym mowa w ust. 1, może przetwarzać dane wyłącznie w zakresie i celu przewidzianym w umowie.

Jak ustalono w toku kontroli, dane osobowe w zakresie: imię, nazwisko i adres e-mail, pozyskane za pomocą formularza kontaktowego sklepu internetowego [...] przekazywane są na skrzynkę poczty elektronicznej o adresie [...]. Ww. skrzynka poczty elektronicznej została założona poprzez rejestrację konta w G. S.A. Jednocześnie ze zgromadzonego w sprawie materiału dowodowego wynika, iż Spółka nie zawarła z G. S.A. pisemnej umowy powierzenia przetwarzania danych osobowych w związku z korzystaniem z poczty elektronicznej.

W toku kontroli ustalono ponadto, iż Spółka przekazuje dane osobowe klientów w zakresie: imię, nazwisko, nazwa prowadzonej działalności gospodarczej, adres oraz Numer Identyfikacji Podatkowej, znajdujące się na fakturach VAT, Pani A. F., w związku z umową o prowadzenie księgowości zawartą w dniu [...] listopada 2012 r. Wskazana umowa nie zawiera zakresu i celu przetwarzania danych osobowych, co stanowi *essentialia negotii* umowy powierzenia przetwarzania danych osobowych, o której mowa w art. 31 ust. 1 ustawy. Wobec powyższego brak jest podstaw do uznania wskazanej umowy za umowę powierzenia przetwarzania danych osobowych, o której mowa w art. 31 ust. 1 ustawy.

Przeprowadzona kontrola wykazała również, iż baza danych klientów sklepu internetowego [...] znajduje się na serwerze należącym do O. Sp. z o.o. Ustalono, iż wskazany podmiot posiada dostęp do wszystkich danych osobowych przetwarzanych z wykorzystaniem ww. serwera, jednakże Spółka nie zawarła z O. Sp. z o.o. pisemnej umowy dotyczącej powierzenia przetwarzania danych osobowych.

Jednocześnie ustalono, iż Spółka zleciła administrowanie serwerem, na którym znajduje się baza danych klientów sklepu internetowego [...] Panu G. P., na podstawie umowy [...] z dnia [...] października 2013 r. W związku z wykonywaniem ww. umowy Pan G. P. posiada dostęp do wszystkich danych osobowych przetwarzanych na serwerze dzierżawionym od O. Sp. z o.o. Wskazana umowa nie zawiera zakresu i celu przetwarzania danych osobowych, co stanowi *essentialia negotii* umowy powierzenia przetwarzania danych osobowych, o której mowa w art. 31

ust. 1 ustawy. Nie można zatem uznać jej za umowę, na podstawie której administrator danych, działając w oparciu o art. zgodnie z art. 31 ust. 1 ustawy, powierza innemu podmiotowi przetwarzanie danych osobowych.

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.

Natomiast zgodnie z wymogami części C pkt XIII załącznika do rozporządzenia, administrator danych stosuje środki kryptograficznej ochrony wobec danych wykorzystywanych do uwierzytelnienia, które są przesyłane w sieci publicznej.

W toku kontroli ustalono, że procesy tworzenia konta przez klienta na stronie sklepu internetowego [...], logowania się na to konto i tworzenia zamówienia towaru, a także cały proces sprzedaży prowadzonej w sklepie internetowym [...] nie są zabezpieczone za pomocą środków ochrony kryptograficznej, tj. bezpiecznego protokołu https. Spółka nie zastosowała zatem odpowiednich środków technicznych i organizacyjnych w celu ochrony danych osobowych przesyłanych w sieci publicznej w związku z realizacją ww. procesów.

Zgodnie z art 41 ust. 2 ustawy, administrator danych jest obowiązany zgłaszać Generalnemu Inspektorowi każdą zmianę informacji, o której mowa w ust. 1, w terminie 30 dni od dnia dokonania zmiany w zbiorze danych. Do zgłaszania zmian stosuje się odpowiednio przepisy o rejestracji zbiorów danych.

Jak ustalono, Spółka zgłosiła do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych zbiór danych osobowych o nazwie S. (zgłoszenie nr [...]). Analiza informacji zawartych w nadesłanym zgłoszeniu zbioru do rejestracji ujawniła rozbieżności pomiędzy informacjami w nim zawartymi a stanem faktycznym ustalonym w wyniku przeprowadzonej kontroli. Wskazane rozbieżności dotyczyły:

a) adresu siedziby administratora danych - w zgłoszeniu zbioru do rejestracji wskazano nieaktualny adres siedziby Spółki, obecny adres siedziby Spółki to [...];

b) przedstawiciela Spółki, o którym mowa w art. 31a ustawy - jak ustalono Spółka jest podmiotem posiadającym siedzibę na terenie Rzeczypospolitej Polskiej, natomiast Pan P. K. wskazany jako przedstawiciel Spółki, o którym mowa w art. 31a, pełni funkcję Prezesa Zarządu Spółki;

c) powierzenia przetwarzania danych osobowych - w zgłoszeniu zbioru do rejestracji nie wskazano, że przetwarzanie danych osobowych zostało powierzone następującym podmiotom: G. S.A., A. F., O. Sp. z o.o. i G. P.;

d) podstawy prawnej przetwarzania danych osobowych - w zgłoszeniu zbioru do rejestracji Spółka wskazała, jako podstawę prawną przetwarzania danych osobowych zgodę osoby, której dane dotyczą oraz fakt, iż przetwarzanie danych jest niezbędne do realizacji uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa. W toku kontroli ustalono jednak, że podstawą prawną przetwarzania danych osobowych jest art. 23 ust. 1 pkt 3 ustawy, który stanowi iż przetwarzanie danych jest dopuszczalne wtedy, gdy jest to konieczne do realizacji umowy, gdy osoba, której dane dotyczą, jest jej stroną lub gdy jest to niezbędne do podjęcia działań przed zawarciem umowy na żądanie osoby, której dane dotyczą oraz art. 23 ust. 1 pkt 5 ustawy, który stanowi iż przetwarzanie danych jest dopuszczalne wtedy, gdy jest ono niezbędne do wypełnienia prawnie usprawiedliwionych celów realizowanych przez administratora danych;

e) zakresu przetwarzanych danych osobowych - Spółka nie wskazała w zgłoszeniu, iż przetwarza także następujące informacje dotyczące klientów: adres e-mail, nazwa prowadzonej działalności gospodarczej, nr użytkownika, nr zamówienia, adres IP.

Należy zatem uznać, iż zgłoszenie zbioru danych osobowych o nazwie S. (nr zgłoszenia: [...]) wymaga aktualizacji w wyżej wskazanym zakresie.

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.).