**GENERALNY INSPEKTOR OCHRONY DANYCH OSOBOWYCH**

*dr Edyta Bielak-Jomaa*

Warszawa, dnia 21 marca 2016 r.

DIS/DEC- 218/16/19879

dot. […]

**D E C Y Z J A**

Na podstawie art. 138 § 1 pkt 1 i pkt 2 ustawy z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego (Dz. U. z 2016 r. poz. 23) oraz art. 12 pkt 2, art. 18 ust. 1 pkt 1 oraz art. 22 w związku z art. 26 ust. 1 pkt 1 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2015 r. poz. 2135, ze zm.), po przeprowadzeniu postępowania administracyjnego w sprawie wniosku A. Sp. z o.o., o ponowne rozpatrzenie sprawy zakończonej decyzją Generalnego Inspektora Ochrony Danych Osobowych z dnia 18 grudnia 2015 r., nr DIS/DEC-967/15/106825, nakazującą usunięcie uchybień w procesie przetwarzania danych osobowych przez A. Sp. z o.o.,

**1. Uchylam zaskarżoną decyzję w części dotyczącej nakazu przywrócenia stanu zgodnego z prawem poprzez zaprzestanie pozyskiwania bez podstawy prawnej, tj. zgody, o której mowa w art. 161 ust. 3 ustawy z dnia 16 lipca 2004 r. Prawo telekomunikacyjne (Dz. U. z 2014 r. poz. 243, z późn. zm.), danych osobowych użytkowników będących osobami fizycznymi w zakresie serii i numeru paszportu oraz w części dotyczącej terminu wykonania nakazu zaskarżonej decyzji i określam termin wykonania nakazu zaskarżonej decyzji do dnia 30 czerwca 2016 r.**

**2. W pozostałym zakresie utrzymuję w mocy zaskarżoną decyzję.**

**Uzasadnienie**

*ul. Stawki 2*
*00-193 Warszawa*

*tel. 22 531 03 13*
*22 531 03 04*
*fax 22 531 03 01*

*www.giodo.gov.pl*

W dniu 18 grudnia 2015 r. Generalny Inspektor Ochrony Danych Osobowych (dalej również „Generalny Inspektor”) wydał decyzję nr DIS/DEC-967/15/106825, nakazującą A. Sp. z o.o. (dalej także: Spółce), jako administratorowi danych, usunięcie uchybień w procesie przetwarzania danych osobowych poprzez zaprzestanie pozyskiwania bez podstawy prawnej, tj. zgody, o której mowa w art. 161 ust. 3 ustawy z dnia 16 lipca 2004 r. Prawo telekomunikacyjne (Dz. U. z 2014 r. poz. 243 z późn. zm.), danych osobowych użytkowników będących osobami fizycznymi w następującym zakresie: kolor oczu, wzrost, wizerunek twarzy, adres zameldowania, nazwa organu wydającego dowód osobisty, data wydania i termin ważności dowodu osobistego, podpis posiadacza dowodu osobistego, seria i numer paszportu, data wydania i data upływu ważności paszportu, nazwa organu wydającego paszport, podpis posiadacza paszportu, nazwa organu wydającego kartę stałego pobytu, data upływu ważności karty stałego pobytu, rodzaj wydanego pozwolenia na pobyt, podpis posiadacza karty stałego pobytu, w terminie 30 dni od dnia, w którym decyzja stanie się ostateczna. W pozostałym zakresie postępowanie umorzono.

W dniu […] stycznia 2016 r. do Biura Generalnego Inspektora Ochrony Danych Osobowych wpłynął, złożony w terminie, wniosek pełnomocnika Spółki o ponowne rozpatrzenie sprawy zakończonej decyzją Generalnego Inspektora Ochrony Danych Osobowych z dnia 18 grudnia 2015 r., nr DIS/DEC-967/15/106825, oraz uchylenie zaskarżonej decyzji i umorzenie postępowania administracyjnego.

Zaskarżonej decyzji zarzucono naruszenie:

1) art. 161 ust. 2 pkt 6 ustawy z dnia 16 lipca 2004 r. Prawo telekomunikacyjne (tj. Dz. U. z 2014 r. poz. 243, z późn. zm.), poprzez bezpodstawne przyjęcie, że Spółka nie ma prawa pozyskiwania bez zgody, o której mowa w art. 161 ust. 3 ustawy Prawo telekomunikacyjne, numeru paszportu użytkownika będącego osobą fizyczną;

2) art. 161 ust. 2 pkt 7 ustawy Prawo telekomunikacyjne poprzez jego błędną wykładnię uznając, że dokumenty potwierdzające tożsamość, w szczególności dowód osobisty lub paszport, nie mogą być uznane za dokumenty potwierdzające możliwość wykonania zobowiązania wobec dostawcy publicznie dostępnych usług telekomunikacyjnych, a w konsekwencji przyjęcie, że dostawca publicznie dostępnych usług telekomunikacyjnych nie ma prawa pozyskiwać bez zgody, o której mowa w art. 161 ust. 3 ustawy Prawo telekomunikacyjne, danych zawartych w dokumentach potwierdzających tożsamość, innych niż enumeratywnie wymienionych w art. 161 ust. 2 pkt 1-6 ustawy Prawo telekomunikacyjne.

We wniosku o ponowne rozpatrzenie sprawy Strona wskazała ponadto m.in., że:

1. Spółka kopiując przy zawieraniu umów o świadczenie usług telekomunikacyjnych dokumenty abonentów potwierdzające ich tożsamość, posiłkuje się art. 161 ust. 2 pkt 7 ustawy Prawo telekomunikacyjne, traktując przywołany przepis jako podstawę prawną istniejącej praktyki. Zdaniem Spółki, dokumenty potwierdzające tożsamość (dowód osobisty, paszport), podobnie jak inne usankcjonowane przepisami dokumenty wymagane przy zawarciu umowy o świadczenie usług telekomunikacyjnych, są dokumentami potwierdzającymi możliwość wykonania zobowiązania wobec Spółki. Skopiowanie dokumentów potwierdzających tożsamość w znacznym stopniu zmniejsza ryzyko niewykonania zobowiązania przez abonenta, gdyż minimalizuje ryzyko nadużycia, zmniejsza prawdopodobieństwo posługiwania się przez abonenta cudzymi danymi oraz znacznie usprawnia windykację należności (co również jest drogą wykonania zobowiązania wobec dostawcy usług). Ustawodawca nie określając w przepisie, jakie dokumenty mają potwierdzać możliwość wykonania zobowiązania, pozostawił taką decyzję dostawcy usług telekomunikacyjnych. Z tego też względu Spółka traktuje dokumenty potwierdzające tożsamość również jako dokumenty potwierdzające możliwość wykonania zobowiązania i na tej podstawie z mocy ustawy przetwarza dane abonentów zawarte w tych dokumentach.

2. Potencjalne skutki decyzji administracyjnej zabraniającej dostawcy usług telekomunikacyjnych przetwarzania danych wykraczających poza zakres wskazany w art. 161 ust. 2 pkt 1-6, zawartych w dokumentach potwierdzających tożsamość, to: zwiększenie liczby nadużyć, bowiem nieuczciwy klient wiedząc, że dostawca usług telekomunikacyjnych nie będzie kopiował i archiwizował kopii dokumentów tożsamości, będzie miał większą tendencję do posłużenia się fałszywym dokumentem, gdyż nie będzie dowodu na jego przestępczy proceder; trudności windykacyjne, z uwagi na to, że dostawca usług telekomunikacyjnych nie będzie miał dowodu dla sądu czy prokuratora, potwierdzającego fakt, że przedłożono mu fałszywy dokument tożsamości; ograniczenie istniejącej obecnie ścisłej kontroli nad nieuczciwymi pracownikami salonów firmowych i autoryzowanymi przedstawicielami i zwiększenie tendencji do trudnych do udowodnienia nadużyć polegających na zawieraniu fałszywych umów w celu wyłudzenia sprzętu; zwiększenie liczby naruszeń danych osobowych w rozumieniu art. 174a ustawy Prawo telekomunikacyjne.

3. Zgodnie z art. 7 pkt 2 ustawy o ochronie danych osobowych, przetwarzanie danych to jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te które wykonuje się w systemach informatycznych. Konsultant, któremu przedstawiono dokument do wglądu przetwarza zatem każdorazowo wszystkie dane w nim zawarte, w tym również dane zakwestionowane przez GIODO. Z punktu widzenia przepisów ustawy o ochronie danych osobowych istotny jest nie sam fakt kopiowania dokumentów, lecz to by gromadzenie danych zawartych w kopiach tych dokumentów

było oparte na konkretnej podstawie prawnej. Dokonywana przez GIODO literalna interpretacja przepisów prowadzi w konsekwencji do braku możliwości weryfikacji przez konsultantów Spółki jakichkolwiek dokumentów potwierdzających tożsamość, bez względu na to, czy byłyby następnie kopiowane czy też nie.

4. Pozyskiwanie przez Spółkę kserokopii dokumentów potwierdzających tożsamość nie prowadzi do pozyskiwania danych osobowych w postaci numeru paszportu, wykraczających poza zakres wskazany w art. 161 ust. 2 ustawy Prawo telekomunikacyjne, bowiem zgodnie z art. 161 ust. 2 pkt 6 ww. ustawy, dostawca publicznie dostępnych usług telekomunikacyjnych jest uprawniony do przetwarzania danych dotyczących użytkownika będącego osobą fizyczną w zakresie nazwy, serii i numeru dokumentów potwierdzających tożsamość, a w przypadku cudzoziemca, który nie jest obywatelem państwa członkowskiego albo Konfederacji Szwajcarskiej - numeru paszportu lub karty pobytu.

5. Termin realizacji decyzji z dnia 18 grudnia 2015 r. określony przez Generalnego Inspektora na 30 dni, jest zbyt krótki ze względu na konieczność wprowadzenia zmian w różnych kanałach sprzedaży, wielu procesach biznesowych i systemach informatycznych, a także umowach i procedurach operacyjnych dotyczących współpracy z partnerami biznesowymi. W ocenie Spółki realny okres na ewentualne wprowadzenie zmian w tym zakresie wynosi minimum 3 miesiące.

Generalny Inspektor Ochrony Danych Osobowych, po ponownym rozpatrzeniu sprawy, zważył co następuje:

Zgodnie z art. 26 ust. 1 pkt 1 ustawy, administrator danych przetwarzający dane powinien dołożyć szczególnej staranności w celu ochrony interesów osób, których dane dotyczą, a w szczególności jest obowiązany zapewnić, aby dane te były przetwarzane zgodnie z prawem. Stosownie zaś do art. 57 ust. 1 pkt 3 Prawa telekomunikacyjnego, dostawca publicznie dostępnych usług telekomunikacyjnych nie może uzależniać zawarcia umowy o świadczenie publicznie dostępnych usług telekomunikacyjnych, w tym o zapewnienie przyłączenia do publicznej sieci telekomunikacyjnej, od udzielenia informacji lub danych, innych niż określone w art. 161 ust. 2, w przypadku użytkownika końcowego będącego osobą fizyczną. Natomiast w myśl art. 161 ust. 2 ustawy Prawo telekomunikacyjne, dostawca publicznie dostępnych usług telekomunikacyjnych jest uprawniony do przetwarzania następujących danych dotyczących użytkownika będącego osobą fizyczną: 1) nazwisk i imion; 2) imion rodziców; 3) miejsca i daty urodzenia; 4) adresu miejsca zamieszkania i adresu korespondencyjnego jeżeli jest on inny niż adres miejsca zamieszkania; 5) numeru ewidencyjnego PESEL - w przypadku obywatela Rzeczypospolitej Polskiej; 6) nazwy, serii i numeru dokumentów potwierdzających tożsamość, a w przypadku cudzoziemca, który nie

jest obywatelem państwa członkowskiego albo Konfederacji Szwajcarskiej - numeru paszportu lub karty pobytu; 7) zawartych w dokumentach potwierdzających możliwość wykonania zobowiązania wobec dostawcy publicznie dostępnych usług telekomunikacyjnych wynikającego z umowy o świadczenie usług telekomunikacyjnych. Oprócz danych, o których mowa w ust. 2, dostawca publicznie dostępnych usług telekomunikacyjnych może, za zgodą użytkownika będącego osobą fizyczną, przetwarzać inne dane tego użytkownika w związku ze świadczoną usługą, w szczególności numer konta bankowego lub karty płatniczej, a także adres poczty elektronicznej oraz numery telefonów kontaktowych (art. 161 ust. 3 ustawy Prawo telekomunikacyjne). Zgodnie z art. 174 pkt 1 ustawy Prawo telekomunikacyjne, jeżeli przepisy ustawy wymagają wyrażenia zgody przez abonenta lub użytkownika końcowego, zgoda ta nie może być domniemana lub dorozumiana z oświadczenia woli o innej treści.

W toku kontroli ustalono, że Spółka osobom zainteresowanym jej ofertą udostępnia trzy kanały sprzedaży, za pośrednictwem których można zawrzeć ze Spółką umowę o świadczenie usług telekomunikacyjnych, tj. kanał stacjonarny (punkty sprzedaży), kanał internetowy (strona […] lub […]) oraz kanał telefoniczny (telefoniczne centrum obsługi). W każdym z ww. kanałów sprzedaży obowiązują procedury regulujące proces zawierania umowy, w tym określające sposób weryfikacji tożsamości klienta w procesie zawierania umowy. Zgodnie z obowiązującymi w Spółce procedurami, w procesie zawierania umowy o świadczenie usług telekomunikacyjnych za pośrednictwem każdego z ww. kanałów sprzedaży Spółka pozyskuje od klientów indywidualnych oraz klientów będących osobami fizycznymi prowadzącymi działalność gospodarczą kopie dokumentów potwierdzających tożsamość. W przypadku, gdy umowa jest zawierana z osobą fizyczną będącą obywatelem polskim wymagana jest kopia obu stron dowodu osobistego klienta, a przypadku cudzoziemca – paszport (kopiowaniu podlega strona z numerem seryjnym dokumentu, zdjęciem, danymi osobowymi klienta oraz datą ważności) lub dowód osobisty z UE oraz karta stałego pobytu.

W toku kontroli wyjaśniono, że wszystkie dokumenty pozyskiwane w procesie zawierania umowy o świadczenie usług telekomunikacyjnych, w tym dokumenty potwierdzające tożsamość, Spółka traktuje jako dokumenty potwierdzające możliwość wykonania zobowiązania i z tego też względu z mocy ustawy Prawo telekomunikacyjne, tj. w oparciu o jej art. 161 ust. 2 pkt 7, przetwarza dane abonentów zawarte w kopiach tych dokumentów. Z ustaleń kontroli wynika również, że Spółka nie pozyskuje zgody, o której mowa w art. 161 ust. 3 ustawy Prawo telekomunikacyjne, na przetwarzanie danych osobowych zawartych w przekazanych Spółce przez klientów dla celów zawarcia umowy o świadczenie usług telekomunikacyjnych kopiach

dokumentów, a wykraczających poza zakres określony w art. 161 ust. 2 ustawy Prawo telekomunikacyjne.

We wniosku o ponowne rozpatrzenie sprawy pełnomocnik Spółki ponownie wskazał, że w ocenie Spółki dokumenty potwierdzające tożsamość (dowód osobisty, paszport), jak i inne usankcjonowane przepisami dokumenty wymagane przy zawarciu umowy oświadczenie usług telekomunikacyjnych, są dokumentami potwierdzającymi możliwość wykonania zobowiązania wobec Spółki. Pozyskanie przez Spółkę kserokopii dokumentów potwierdzających tożsamość zmniejsza bowiem w znacznym stopniu ryzyko niewykonania zobowiązania przez abonenta, minimalizując ryzyko nadużycia, zmniejsza prawdopodobieństwo posługiwania się przez abonenta cudzymi danymi oraz znacznie usprawnia windykację należności, co również jest drogą wykonania zobowiązania wobec dostawcy usług. Podstawę prawną kopiowania przez Spółkę dokumentów potwierdzających tożsamość abonentów stanowi art. 161 ust. 2 pkt 7 ustawy Prawo telekomunikacyjne. Ustawodawca nieokreślając, jakie dokumenty mają potwierdzać możliwość wykonania zobowiązania, pozostawił taką decyzję dostawcy usług telekomunikacyjnych. Z tego też względu Spółka traktuje dokumenty potwierdzające tożsamość również jako dokumenty potwierdzające możliwość wykonania zobowiązania i na tej podstawie z mocy ustawy przetwarza dane abonentów zawarte w tych dokumentach.

Odnosząc się do powyższego należy wskazać, że w art. 161 ust. 2 pkt 1-6 ustawy Prawo telekomunikacyjne określony został katalog danych identyfikujących użytkownika będącego osobą fizyczną, do przetwarzania których uprawniony jest dostawca publicznie dostępnych usług telekomunikacyjnych. Danymi tymi są: 1) nazwisko i imiona; 2) imiona rodziców; 3) miejsce i data urodzenia; 4) adres miejsca zamieszkania i adres korespondencyjny jeżeli jest on inny niż adres miejsca zamieszkania; 5) numer ewidencyjny PESEL - w przypadku obywatela Rzeczypospolitej Polskiej; 6) nazwa, seria i numer dokumentów potwierdzających tożsamość, a w przypadku cudzoziemca, który nie jest obywatelem państwa członkowskiego albo Konfederacji Szwajcarskiej - numer paszportu lub karty pobytu. Natomiast art. 161 ust. 2 pkt 7 ustawy Prawo telekomunikacyjne uprawnia dostawcę publicznie dostępnych usług telekomunikacyjnych do przetwarzania danych dotyczących użytkownika będącego osobą fizyczną zawartych w dokumentach potwierdzających możliwość wykonania zobowiązania wobec dostawcy publicznie dostępnych usług telekomunikacyjnych wynikającego z umowy o świadczenie usług telekomunikacyjnych.

Wobec powyższego należy wskazać, że kwestia zakresu danych służących identyfikacji użytkownika będącego osobą fizyczną, do przetwarzania których uprawniony jest dostawca publicznie dostępnych usług telekomunikacyjnych, została rozstrzygnięta w art. 161 ust. 2 pkt 1-6 ustawy Prawo telekomunikacyjne. Z tego też względu treść art. 161 ust. 2 pkt 7 ww. ustawy należy

rozumieć w sposób ścisły i zgodny z celem tego przepisu, którym jest stworzenie podstawy prawnej umożliwiającej dostawcy publicznie dostępnych usług telekomunikacyjnych przetwarzanie, obok danych identyfikujących użytkownika, również danych zawartych w dokumentach służących ustaleniu, czy użytkownik będzie w stanie wykonać zobowiązanie względem dostawcy publicznie dostępnych usług telekomunikacyjnych.

Podkreślenia w tym miejscu wymaga, że konsekwencją przyjęcia proponowanej przez Spółkę interpretacji art. 161 ust. 2 pkt 7 ustawy Prawo telekomunikacyjne, zgodnie z którą ww. przepis uprawnia dostawcę usług do przetwarzania danych zawartych w dowodzie osobistym, byłoby pozbawienie znaczenia, zawartego w art. 161 ust. 2 pkt 1-6 ustawy Prawo telekomunikacyjne unormowania, tworzącego katalog danych identyfikujących użytkownika końcowego, do przetwarzania których z mocy ustawy uprawniony jest dostawca publicznie dostępnych usług telekomunikacyjnych.

W związku z tym, że zobowiązanie użytkownika polega na zapłacie należności pieniężnej, działając na podstawie art. 161 ust. 2 pkt 7 ustawy Prawo telekomunikacyjne, dostawca usług może pozyskiwać dokumenty potwierdzające zdolność do wykonania zobowiązania pieniężnego i przetwarzać dane zawarte w tych dokumentach. Zgodnie zaś z art. 4 ust. 1 ustawy z dnia 6 sierpnia 2010 r. o dowodach osobistych (Dz. U. z 2010 r. Nr 167 poz. 1131, ze zm.), dowód osobisty jest dokumentem stwierdzającym tożsamość i obywatelstwo polskie, a w myśl art. 4 ustawy z dnia 13 lipca 2006 r. o dokumentach paszportowych (Dz. U. z 2013 r. poz. 268, ze zm.), dokument paszportowy uprawnia do przekraczania granicy i pobytu za granicą oraz poświadcza obywatelstwo polskie, a także tożsamość osoby w nim wskazanej w zakresie danych, jakie ten dokument zawiera. Ponadto, zgodnie z art. 242 ustawy o cudzoziemcach (Dz. U. z 2013 r. poz. 1650, ze zm.), karta pobytu w okresie swojej ważności potwierdza tożsamość cudzoziemca podczas jego pobytu na terytorium Rzeczypospolitej Polskiej oraz uprawnia go, wraz z dokumentem podróży, do wielokrotnego przekraczania granicy bez konieczności uzyskania wizy. Wobec powyższego, dane zawarte w dokumentach takich jak dowód osobisty, paszport, karta pobytu, służą identyfikacji osoby. Ww. dokumenty nie zawierają informacji, które pozwalałyby na dokonanie oceny, czy użytkownik będzie w stanie wykonać zobowiązanie pieniężne względem dostawcy publicznie dostępnych usług telekomunikacyjnych. Z powyższych względów dokumenty potwierdzające tożsamość takie jak: dowód osobisty, paszport, karta pobytu, nie są dokumentami, które potwierdzałyby możliwość wykonania zobowiązania wobec dostawcy publicznie dostępnych usług telekomunikacyjnych wynikającego z umowy o świadczenie usług telekomunikacyjnych. Tym samym art. 161 ust. 2 pkt 7 ustawy Prawo telekomunikacyjne nie stanowi podstawy prawnej do przetwarzania danych w nich zawartych.

Zgodnie z art. 12 ustawy z dnia 6 sierpnia 2010 r. o dowodach osobistych (Dz. U. z 2010 r. Nr 167, poz. 1131 ze zm.), w dowodzie osobistym zamieszcza się następujące dane: nazwisko, imię (imiona), nazwisko rodowe, imiona rodziców, datę i miejsce urodzenia, płeć, wizerunek twarzy, numer PESEL, obywatelstwo, serię i numer dowodu osobistego, datę wydania, datę ważności, oznaczenie organu wydającego dowód osobisty. Wzór dowodu osobistego został określony w załączniku nr 1 do rozporządzenia Ministra Spraw Wewnętrznych z dnia 16 lutego 2015 r. w sprawie wzoru dowodu osobistego oraz sposobu i trybu postępowania w sprawach wydawania dowodów osobistych, ich utraty, uszkodzenia, unieważnienia i zwrotu (Dz. U. poz. 212). Ponadto, zgodnie z art. 88 ww. ustawy, dowody osobiste wydane przed dniem 1 marca 2015 r. zachowują ważność do upływu terminów w nich określonych. Art. 37 ust. 1 i ust. 2 poprzednio obowiązującej ustawy z dnia 10 kwietnia 1974 r. o ewidencji ludności i dowodach osobistych (Dz. U. z 2006 r. Nr 139, poz. 993, ze zm.), uchylonej ustawą z dnia 6 sierpnia 2010 r. o dowodach osobistych, określał następujący zakres danych zamieszczanych w dowodzie osobistym: nazwisko, nazwisko rodowe i imię (imiona); imiona rodziców; data i miejsce urodzenia; adres miejsca zameldowania na pobyt stały; płeć; wzrost w centymetrach; kolor oczu; wizerunek twarzy; numer PESEL; nazwa organu wydającego dowód osobisty; datę wydania i termin ważności; seria i numer dowodu osobistego oraz podpis jego posiadacza (art. 37 ust. 2 ww. ustawy). W myśl art. 18 ust. 1 ustawy z dnia 13 lipca 2006 r. o dokumentach paszportowych (Dz. U. z 2013 r. poz. 268, ze zm.), w dokumencie paszportowym zamieszcza się następujące dane: nazwisko, imię (imiona), datę i miejsce urodzenia, obywatelstwo, płeć, wizerunek twarzy i podpis posiadacza, datę wydania i datę upływu ważności dokumentu paszportowego, serię i numer dokumentu paszportowego, numer PESEL, nazwę organu wydającego oraz dane biometryczne (umieszczone w dokumentach paszportowych w formie elektronicznej zgodnie z art. 2 pkt 1 powołanej ustawy). Wzór paszportu został określony w załączniku nr 1 do rozporządzenia Ministra Spraw Wewnętrznych z dnia 16 lutego 2015 r. w sprawie dokumentów paszportowych (Dz. U. z 2010 r. nr 152, poz. 1026). Stosownie zaś do art. 244 ust. 1 ustawy o cudzoziemcach (Dz. U. z 2013 r. poz. 1650, ze zm.), w karcie pobytu umieszcza się: imię (imiona) i nazwisko cudzoziemca oraz imiona rodziców, datę, miejsce i kraj urodzenia, adres zameldowania na pobyt stały lub czasowy, informację o obywatelstwie, informację o płci, informację o wzroście w centymetrach i kolorze oczu, numer ewidencyjny Powszechnego Elektronicznego Systemu Ewidencji Ludności (PESEL) - w przypadku gdy został nadany, informację o rodzaju udzielonego zezwolenia, adnotację „naukowiec” – w przypadku zezwolenia, o którym mowa w art. 151, adnotację „Niebieska Karta UE” – w przypadku zezwolenia, o którym mowa w art. 127, adnotację „dostęp do rynku pracy” – w przypadku zezwolenia udzielonego cudzoziemcowi, który jest uprawniony do wykonywania pracy na terytorium Rzeczypospolitej

Polskiej lub jest zwolniony z obowiązku posiadania zezwolenia na pracę, adnotację „Poprzednio posiadacz Niebieskiej Karty UE” - w przypadku zezwolenia na pobyt rezydenta długoterminowego UE udzielonego cudzoziemcowi, któremu udzielono zezwolenia na pobyt czasowy w celu wykonywania pracy w zawodzie wymagającym wysokich kwalifikacji, obraz linii papilarnych, nazwę organu wydającego kartę, datę wydania karty, datę upływu okresu ważności karty, fotografię cudzoziemca, adnotację „ochrona międzynarodowa przyznana przez ... (wskazanie państwa członkowskiego Unii Europejskiej, które ją przyznało) w dniu ... (data przyznania ochrony międzynarodowej)” – w przypadku zezwolenia na pobyt rezydenta długoterminowego UE udzielonego cudzoziemcowi, któremu przyznano ochronę międzynarodową. Zgodnie z ust. 2 ww. przepisu, niezależnie od danych, o których mowa w ust. 1, karta pobytu może zawierać podpis cudzoziemca oraz zakodowany zapis danych, o których mowa w ust. 1 pkt 1, 2, 4, 5 lub 16. Zgodnie ze wzorem karty pobytu określonym w załączniku nr 1 do rozporządzenia Ministra Spraw Wewnętrznych z dnia 29 kwietnia 2014 r. w sprawie dokumentów wydawanych cudzoziemcom (Dz. U. z 2014 r. poz. 589), na karcie pobytu zamieszcza się następujące dane: nazwisko i imiona, imiona rodziców, data i miejsce urodzenia, PESEL, adres zameldowania, obywatelstwo, wizerunek, wzrost, płeć, kolor oczu, podpis posiadacza, nazwa organu wydającego kartę, rodzaj wydanego zezwolenia na pobyt, data upływu ważności karty.

Z powyższego wynika, że pozyskiwanie przez Spółkę kopii dokumentów potwierdzających tożsamość (dowodów osobistych, paszportów, kart stałego pobytu), prowadzi do pozyskiwania danych osobowych wykraczających poza zakres wskazany w art. 161 ust. 2 ustawy Prawo telekomunikacyjne, takich jak: kolor oczu, wzrost (w centymetrach), wizerunek twarzy, adres zameldowania, nazwa organu wydającego dowód osobisty, data wydania i termin ważności dowodu osobistego, podpis posiadacza dokumentu, nazwa organu wydającego kartę stałego pobytu, data upływu ważności karty stałego pobytu, rodzaj wydanego pozwolenia na pobyt, data wydania i data upływu ważności dokumentu paszportowego, nazwa organu wydającego paszport.

Zgodnie z art. 161 ust. 3 ustawy Prawo telekomunikacyjne, oprócz danych, o których mowa w ust. 2, dostawca publicznie dostępnych usług telekomunikacyjnych może, za zgodą użytkownika będącego osobą fizyczną, przetwarzać inne dane tego użytkownika w związku ze świadczoną usługą, w szczególności numer konta bankowego lub karty płatniczej, a także adres poczty elektronicznej oraz numery telefonów kontaktowych.

Jak wynika z ustaleń kontroli, Spółka nie pozyskuje zgody, o której mowa w art. 161 ust. 3 ustawy Prawo telekomunikacyjne, na przetwarzanie danych osobowych zawartych w przekazanych Spółce przez klientów dla celów zawarcia umowy o świadczenie usług telekomunikacyjnych

kopiach dokumentów potwierdzających tożsamość, a wykraczających poza zakres określony w art. 161 ust. 2 ustawy Prawo telekomunikacyjne.

W związku z powyższym należy stwierdzić, że brak jest podstawy prawnej do przetwarzania przez Spółkę danych osobowych zawartych w kopiach dokumentów potwierdzających tożsamość, a wykraczających poza zakres wskazany w art. 161 ust. 2 ustawy Prawo telekomunikacyjne, takich jak: kolor oczu, wzrost (w centymetrach), wizerunek twarzy, adres zameldowania, nazwa organu wydającego dowód osobisty, data wydania i termin ważności dowodu osobistego, podpis posiadacza dokumentu, nazwa organu wydającego kartę stałego pobytu, data upływu ważności karty stałego pobytu, rodzaj wydanego pozwolenia na pobyt, data wydania i data upływu ważności dokumentu paszportowego, nazwa organu wydającego paszport.

We wniosku o ponowne rozpatrzenie sprawy pełnomocnik Spółki wskazał, że przyjęcie prezentowanej przez Generalnego Inspektora interpretacji art. 161 ust. 2 pkt 7 ustawy Prawo telekomunikacyjne, niesie za sobą ryzyko zwiększenia liczby nadużyć ze strony nieuczciwych klientów, bowiem wiedząc, że dostawca usług telekomunikacyjnych nie będzie kopiował i archiwizował kopii dokumentów tożsamości, będą oni mieli większą tendencję do posłużenia się fałszywym dokumentem; trudności windykacyjne (dostawca usług telekomunikacyjnych nie będzie miał dowodu dla sądu czy prokuratora potwierdzającego fakt, że przedłożono mu fałszywy dokument tożsamości); ograniczenie istniejącej obecnie ścisłej kontroli nad nieuczciwymi pracownikami salonów firmowych i autoryzowanymi przedstawicielami i zwiększenie tendencji do trudnych do udowodnienia nadużyć polegających na zawieraniu fałszywych umów w celu wyłudzenia sprzętu; zwiększenie liczby naruszeń danych osobowych w rozumieniu art. 174a ustawy Prawo telekomunikacyjne.

Odnosząc się do powyższego należy wskazać, że Spółka dobierając środki i metody zapobiegania ww. nadużyciom powinna działać w granicach obowiązującego prawa. Stosowanie środków zapobiegania nadużyciom, które prowadzą do naruszenia istniejących regulacji prawnych w zakresie przetwarzania danych osobowych, jest zatem niedopuszczalne. Jak wyżej wskazano, Spółka pozyskując i archiwizując kopie dokumentów potwierdzających tożsamość klientów w procesie zawierania umowy o świadczenie usług telekomunikacyjnych pozyskuje bez podstawy prawnej dane osobowe wykraczające poza zakres określony w art. 161 ust. 2 ustawy Prawo telekomunikacyjne.

Odnosząc się natomiast do podniesionego przez Spółkę argumentu, że z punktu widzenia przepisów ustawy o ochronie danych osobowych istotny jest nie sam fakt kopiowania dokumentów, lecz kwestia zgodnego z prawem przetwarzania danych osobowych pozyskiwanych w konsekwencji tej czynności, należy wskazać, że na żadnym z etapów niniejszego postępowania

Generalny Inspektor nie kwestionował samej czynności kopiowania dokumentów, lecz przetwarzanie bez podstawy prawnej danych osobowych wykraczających poza zakres określony w art. 161 ust. 2 ustawy Prawo telekomunikacyjne, przetwarzanych w rezultacie dokonywania kserokopii dokumentów potwierdzających tożsamość.

Ponadto, nie można zgodzić się z poglądem Spółki, że dokonywana przez Generalnego Inspektora interpretacja przepisów w omawianym zakresie prowadzi w konsekwencji do braku możliwości weryfikowania przez konsultantów Spółki jakichkolwiek dokumentów potwierdzających tożsamość klientów, bez względu na to, czy byłyby następnie kopiowane czy też nie, z uwagi na to, że konsultant, któremu przedstawiono dokument do wglądu, przetwarza w rozumieniu art. 7 pkt 2 ustawy o ochronie danych osobowych, każdorazowo wszystkie dane w nim zawarte, w tym również dane zakwestionowane przez Generalnego Inspektora. Należy wskazać bowiem, że sam wgląd w dokument potwierdzający tożsamość, w przypadku, gdy dane w nim zawarte nie są przetwarzane w zbiorze danych, nie prowadzi do ich przetwarzania w rozumieniu ustawy o ochronie danych osobowych. Jak stanowi art. 2 ust. 1 ustawy o ochronie danych osobowych, ustawę stosuje się do przetwarzania danych osobowych w: 1) kartotekach, skorowidzach, księgach, wykazach i innych zbiorach ewidencyjnych, 2) w systemach informatycznych, także w przypadku przetwarzania danych poza zbiorem danych. Wobec powyższego dokonana przez Generalnego Inspektora interpretacja przepisów nie skutkuje brakiem możliwości dokonywania weryfikacji tożsamości klientów Spółki na podstawie okazanego przez klienta dokumentu potwierdzającego tożsamość.

Ponadto, w związku z tym, że zgodnie z art. 161 ust. 2 pkt 6 ww. ustawy, dostawca publicznie dostępnych usług telekomunikacyjnych jest uprawniony do przetwarzania dotyczących użytkownika będącego osobą fizyczną danych w zakresie: nazwy, serii i numeru dokumentów potwierdzających tożsamość, a w przypadku cudzoziemca, który nie jest obywatelem państwa członkowskiego albo Konfederacji Szwajcarskiej - numeru paszportu lub karty pobytu, należy wskazać, iż pozyskiwanie przez Spółkę kserokopii dokumentów potwierdzających tożsamość nie prowadzi do pozyskiwania danych osobowych w postaci numeru paszportu, wykraczających poza zakres wskazany w art. 161 ust. 2 ustawy Prawo telekomunikacyjne, co zostało omyłkowo wskazane w nakazie zaskarżonej decyzji. Wobec powyższego należy uchylić zaskarżoną decyzję w części dotyczącej nakazu przywrócenia stanu zgodnego z prawem poprzez zaprzestanie pozyskiwania bez podstawy prawnej danych osobowych użytkowników będących osobami fizycznymi w zakresie: seria i numer paszportu i umorzyć postępowanie w tym zakresie.

Pełnomocnik Spółki podniósł ponadto, że wyznaczony przez Generalnego Inspektora trzydziestodniowy termin wykonania zaskarżonej decyzji jest zbyt krótki ze względu na konieczność

wprowadzenia przez Spółkę zmian w różnych kanałach sprzedaży, wielu procesach biznesowych i systemach informatycznych, a także w umowach i procedurach operacyjnych dotyczących współpracy z partnerami biznesowymi. Zgodnie z dokonaną przez Spółkę oceną, realny okres na ewentualne wprowadzenie zmian w tym zakresie wynosi minimum 3 miesiące.

Uwzględniając powyższą argumentację Generalny Inspektor Ochrony Danych Osobowych uchylił zaskarżoną decyzję w zakresie dotyczącym terminu jej wykonania i określił nowy termin wykonania nakazu zaskarżonej decyzji.

W tym stanie faktycznym i prawnym, oceniając ponownie zebrany materiał w przedmiotowej sprawie, Generalny Inspektor Ochrony Danych Osobowych rozstrzygnął, jak w sentencji.

Decyzja jest ostateczna. Na podstawie art. 21 ust. 2 ustawy o ochronie danych osobowych w związku z art. 53 § 1 i 54 § 1 ustawy z dnia 30 sierpnia 2002 r. Prawo o postępowaniu przed sądami administracyjnymi (Dz. U. z 2012 r. poz. 270 z późn. zm.), od niniejszej decyzji stronie przysługuje prawo wniesienia skargi do Wojewódzkiego Sądu Administracyjnego w Warszawie, w terminie 30 dni od dnia doręczenia decyzji, za pośrednictwem Generalnego Inspektora Ochrony Danych Osobowych (na adres: ul. Stawki 2, 00-193 Warszawa).

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 2014 r. poz. 1619 ze zm.).