GENERALNY INSPEKTOR OCHRONY DANYCH OSOBOWYCH

dr Edyta Bielak-Jomaa

Warszawa, dnia 18 grudnia 2015 r.

DIS/DEC-967/15/106825

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 ze zm.), 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 2014 r. poz. 1182 ze zm.), po przeprowadzeniu postępowania administracyjnego w sprawie przetwarzania danych osobowych przez A. Sp. z o.o.,

I. Nakazuję A. Sp. z o.o. (dalej również „Spółka"), jako administratorowi danych, przywrócenie 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 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 niniejsza decyzja stanie się ostateczna.

II. W pozostałym zakresie postępowanie umarzam.

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

Upoważniony przez Generalnego Inspektora Ochrony Danych Osobowych inspektor przeprowadził kontrolę w A. Sp. z o.o. 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 ze zm.), zwaną dalej „ustawą". Zakresem kontroli objęto przetwarzanie przez Spółkę danych osobowych klientów Spółki poprzez ustalenie, czy w związku z zawieraniem umów o świadczenie usług telekomunikacyjnych Spółka pozyskuje kopie dokumentów tożsamości klientów Spółki, w tym dowodów osobistych lub innych dokumentów w celu potwierdzenia tożsamości klientów Spółki i czy przetwarza dane osobowe zawarte w tych dokumentach.

W toku kontroli odebrano od pracowników Spółki ustne wyjaśnienia. Stan faktyczny został szczegółowo opisany w protokole kontroli, który został podpisany przez pełnomocnika Spółki (pełnomocnictwo w aktach sprawy).

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 przetwarzaniu bez podstawy prawnej danych osobowych klientów Spółki wykraczających poza zakres wskazany w art. 161 ust. 2 ustawy Prawo telekomunikacyjne, takich jak m.in.: kolor oczu, wzrost (w centymetrach), wizerunek twarzy, płeć, adres zameldowania, nazwa organu wydającego dowód osobisty, data wydania i termin ważności dowodu osobistego, podpis posiadacza dokumentu, dane biometryczne w związku z pozyskiwaniem przez Spółkę kopii dokumentów potwierdzających tożsamość (art. 26 ust. 1 pkt 1 ustawy).

W związku z powyższym Generalny Inspektor Ochrony Danych Osobowych wszczął z urzędu postępowanie administracyjne w niniejszej sprawie w celu wyjaśnienia okoliczności sprawy (sygn. pisma […]).

W odpowiedzi na ww. pismo pełnomocnik Spółki, w piśmie z dnia […] października 2015 r., poinformował, 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 z dnia 16 lipca 2004 r. Prawo telekomunikacyjne (Dz. U. z 2014 r. poz. 243 ze zm.), traktując przywołany przepis jako podstawę prawną istniejącej praktyki. Ustawodawca nie określił w ww. przepisie, jakie dokumenty mają potwierdzać możliwość wykonania zobowiązania, gdyż pozostawił taką decyzję

dostawcy usług telekomunikacyjnych (podobnie Krzysztof Kawałek, Komentarz do art. 161 Pt, Lex: dostawcy usług telekomunikacyjnych pozostawione jest określenie, jakie dokumenty potwierdzają możliwość wykonania zobowiązania użytkownika wobec dostawcy usług telekomunikacyjnych, których to dokumentów dotyczy art. 161 ust. 2 pkt 7.). Zdaniem Spółki, dokumenty potwierdzające tożsamość (dowód osobisty, paszport, karta pobytu), 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).

2. Wszystkie dane dotyczące użytkownika, zgodnie z art. 159 ustawy Prawo telekomunikacyjne, objęte są tajemnicą telekomunikacyjną (nie wyłączając danych zawartych w dokumentach, o których mowa powyżej). Dostawca usług telekomunikacyjnych ma bezwzględny obowiązek ich ochrony, a co za tym idzie, zapewnienie bezpieczeństwa przetwarzania tego typu danych jest istotnym obowiązkiem Spółki, zaś ryzyko wykorzystania ich w innym celu niż świadczenie usług telekomunikacyjnych czy wykonywanie umowy o świadczenie usług telekomunikacyjnych jest znikome.

3. Przyjęcie prezentowanej przez GIODO interpretacji art. 161 ust. 2 pkt 7 ustawy Prawo telekomunikacyjne, niesie za sobą wymierne negatywne skutki dla bezpieczeństwa obrotu gospodarczego na rynku telekomunikacyjnym, nie chroniąc jednocześnie interesu prawnego klientów indywidualnych, gdyż ich dane są i tak ściśle chronione przepisami dotyczącymi tajemnicy telekomunikacyjnej, a potencjalne jej skutki to:

a) zwiększenie liczby nadużyć (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),

b) trudności windykacyjne (dostawca usług telekomunikacyjnych nie będzie miał dowodu dla sądu czy prokuratora, potwierdzającego fakt, że przedłożono mu fałszywy dokument tożsamości),

c) ograniczenie istniejącej obecnie ścisłej kontroli nad nieuczciwymi pracownikami salonów firmowych i autoryzowanymi przedstawicielami (większa tendencja do trudnych do udowodnienia nadużyć polegających na zawieraniu fałszywych umów w celu wyłudzenia sprzętu),

d) zwiększenie liczby naruszeń danych osobowych w rozumieniu art. 174a i nast. ustawy Prawo telekomunikacyjne.

4. Spółka wykonuje kopie paszportów i kart pobytu wykorzystując do tego urządzenia, które nie umożliwiają odczytu danych z użyciem technologii RFID, dlatego też pozyskiwanie przez Spółkę kopii

dokumentów potwierdzających tożsamość nie prowadzi do pozyskiwania danych osobowych w postaci danych biometrycznych, wykraczających poza zakres wskazany w art. 161 ust. 2 ustawy Prawo telekomunikacyjne.

5. Zgodnie z art. 15 ust. 2 ustawy z dnia 24 września 2010 r. o ewidencji ludności (tekst jednolity Dz. U. z 2015 r. poz. 388), numer PESEL to jedenastocyfrowy symbol numeryczny, jednoznacznie identyfikujący osobę fizyczną, zawierający datę urodzenia, numer porządkowy, oznaczenie płci oraz liczbę kontrolną, przy czym numer porządkowy osoby zawarty jest w cyfrach od siódmej do dziesiątej, przy czym ostatnia cyfra numeru porządkowego zawiera oznaczenie płci: cyfrę parzystą (w tym „0") dla kobiet, a cyfrę nieparzystą dla mężczyzn. Biorąc powyższe pod uwagę należy uznać, że pozyskiwanie przez Spółkę kserokopii dokumentów potwierdzających tożsamość nie prowadzi do pozyskiwania danych osobowych, w postaci płci, wykraczających poza zakres wskazany w art. 161 ust. 2 ustawy Prawo telekomunikacyjne.

Po zapoznaniu się z całością materiału dowodowego zebranego w sprawie Generalny Inspektor Ochrony Danych Osobowych 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 udostępnia osobom zainteresowanym ofertą Spółki 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 tych 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, tj. w przypadku, gdy umowa jest zawierana z osobą fizyczną będącą obywatelem polskim wymagana jest kopia dowodu osobistego klienta (obu stron), a przypadku cudzoziemca – paszport (kopiowaniu podlega wyłącznie 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, tj. w oparciu o art. 161 ust. 2 pkt 7 ustawy Prawo telekomunikacyjne, przetwarza dane abonentów zawarte w kopiach tych dokumentów. W piśmie z dnia […] października 2015 r. pełnomocnik Spółki wskazał, że ustawodawca nie określił w ww. przepisie, jakie dokumenty mają potwierdzać możliwość wykonania zobowiązania i pozostawił taką decyzję dostawcy usług telekomunikacyjnych. Zdaniem Spółki, dokumenty potwierdzające tożsamość (dowód osobisty, paszport, karta pobytu), 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).

Ponadto z ustaleń kontroli wynika, 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.

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

W związku z tym, że zobowiązanie użytkownika polega na zapłacie należności pieniężnej, dostawca usług może pozyskiwać dokumenty potwierdzające zdolność do wykonania zobowiązania

pieniężnego i przetwarzać dane zawarte w tych dokumentach. Zgodnie natomiast 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 tych też 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, a tym samym art. 161 ust. 2 pkt 7 ustawy Prawo telekomunikacyjne nie stanowi podstawy prawnej do przetwarzania danych w nim zawartych.

Zgodnie natomiast 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; datę i miejsce urodzenia; adres miejsca zameldowania na pobyt stały; płeć; wzrost w centymetrach; kolor oczu; wizerunek twarzy; numer PESEL; nazwę organu wydającego dowód osobisty; datę wydania i termin ważności; serię 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 natomiast 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.

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, iż brak jest podstaw prawnych 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.

W piśmie z dnia […] października 2015 r. pełnomocnik Spółki wskazał, że przyjęcie prezentowanej przez GIODO interpretacji art. 161 ust. 2 pkt 7 ustawy Prawo telekomunikacyjne, niesie za sobą ryzyko zwiększenia liczby nadużyć ze strony nieuczciwych klientów, którzy wiedząc, że dostawca usług telekomunikacyjnych nie przechowuje kopii ich dokumentów tożsamości, będzie miał większą tendencję do posłużenia się fałszywym dokumentem, gdyż nie będzie dowodu na jego przestępczy proceder), trudności windykacyjne (dostawca usług telekomunikacyjnych nie będzie miał dowodu dla sądu czy prokuratora, potwierdzającego fakt, że przedłożono mu fałszywy dokument tożsamości), a ponadto doprowadzi do ograniczenia istniejącej obecnie ścisłej kontroli nad nieuczciwymi pracownikami i salonów firmowych i autoryzowanymi przedstawicielami, co może doprowadzić do większej tendencji do trudnych do udowodnienia nadużyć polegających na zawieraniu fałszywych umów w celu wyłudzenia sprzętu oraz zwiększenie liczby naruszeń danych osobowych w rozumieniu art. 174a i następnych ustawy Prawo telekomunikacyjne.

Odnosząc się do powyższego należy wskazać, że w granicach obowiązującego prawa Spółka ma swobodę doboru środków i metod zapobiegania wyżej wskazanym nadużyciom.

Niedopuszczalne jest zatem stosowanie takich środków i metod zapobiegania powyższym nadużyciom, które prowadzą do naruszenia istniejących regulacji prawnych w zakresie przetwarzania danych osobowych. Pozyskiwanie i archiwizowanie przez Spółkę kopii dokumentów potwierdzających tożsamość klientów w procesie zawierania umowy o świadczenie usług telekomunikacyjnych prowadzi natomiast do pozyskiwania danych osobowych wykraczających poza zakres określony w art. 161 ust. 2 pkt 1-6 ustawy Prawo telekomunikacyjne, a ponadto może stwarzać ryzyko nieuprawnionego wykorzystania kopii dokumentu tożsamości, w tym zawartych w niej danych osobowych, w przypadku, gdy dostęp do kopii dokumentu faktycznie uzyska osoba nieuczciwa.

Ponadto należy uwzględnić wyjaśnienia pełnomocnika Spółki, z których wynika, że Spółka wykonuje kopie paszportów i kart stałego pobytu wykorzystując do tego urządzenia, które nie umożliwiają odczytu danych z użyciem technologii RFID, dlatego też pozyskiwanie przez Spółkę kopii dokumentów potwierdzających tożsamość nie prowadzi do pozyskiwania danych osobowych w postaci danych biometrycznych umieszczonych w dokumentach paszportowych w formie elektronicznej, wykraczających poza zakres wskazany w art. 161 ust. 2 ustawy Prawo telekomunikacyjne. Uwzględniając powyższe należy uznać, że Spółka nie pozyskuje danych biometrycznych umieszczonych w dokumentach paszportowych w formie elektronicznej i w tym zakresie postępowanie należy umorzyć.

Ponadto należy uwzględnić wyjaśnienia pełnomocnika Spółki, z których wynika, że pozyskiwanie przez Spółkę kopii dokumentów potwierdzających tożsamość nie prowadzi do pozyskiwania danych osobowych w postaci płci, wykraczających poza zakres wskazany w art. 161 ust. 2 ustawy Prawo telekomunikacyjne, z uwagi na to, że Spółka jest uprawniona do pozyskiwania danych w zakresie numeru PESEL, a stosownie do art. 15 ust. 2 ustawy z dnia 24 września 2010 r. o ewidencji ludności (tekst jednolity Dz. U. z 2015 r. poz. 388), numer PESEL to jedenastocyfrowy symbol numeryczny, jednoznacznie identyfikujący osobę fizyczną, zawierający datę urodzenia, numer porządkowy, oznaczenie płci oraz liczbę kontrolną, przy czym numer porządkowy osoby zawarty jest w cyfrach od siódmej do dziesiątej, przy czym ostatnia cyfra numeru porządkowego zawiera oznaczenie płci: cyfrę parzystą (w tym „0”) dla kobiet, a cyfrę nieparzystą dla mężczyzn.

Biorąc powyższe pod uwagę należy uznać, że w związku z tym, iż numer PESEL, do pozyskiwania którego Spółka jest uprawniona, zawiera w sobie informację na temat płci, pozyskiwanie przez Spółkę informacji na temat płci użytkownika, nie prowadzi do przetwarzania danych w zakresie wykraczającym poza zakres danych określony w art. 161 ust. 2 ustawy Prawo telekomunikacyjne. W związku z powyższym zarzut dotyczący pozyskiwania przez Spółkę bez podstawy prawnej danych użytkowników będących osobami fizycznymi w zakresie informacji na temat płci, należy uznać za bezprzedmiotowy i postępowanie w tym zakresie należy umorzyć.

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).

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.).