



**GENERALNY INSPEKTOR
OCHRONY DANYCH
OSOBOWYCH**

dr Edyta Bielak - Jomaa

Warszawa, dnia 15 grudnia 2015 r.

DIS/DEC-955/15/105874

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 ze zm.), art. 12 pkt 2, art. 18 ust. 1 pkt 1, 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 z późn. zm.), po przeprowadzeniu postępowania administracyjnego w sprawie przetwarzania danych osobowych przez P. Sp. z o.o.,

nakazuję P. Sp. z o.o., jako administratorowi danych, przywrócenie stanu zgodnego z prawem poprzez: zaprzestanie przetwarzania 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 końcowych wykraczających poza zakres określony w art. 161 ust. 2 ustawy Prawo telekomunikacyjne (zgodnie z którym oprócz danych, o których mowa w art. 161 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, spełniającej wymogi określone w art. 174 pkt 1 tejże ustawy, w myśl którego, jeżeli przepisy ustawy Prawo telekomunikacyjne wymagają wyrażenia zgody przez abonenta lub użytkownika końcowego, zgoda ta nie może być domniemana lub dorozumiana z oświadczenia woli o innej treści), w następującym zakresie: kolor oczu, wzrost, wizerunek twarzy, płeć, adres zameldowania, nazwę organu wydającego dowód osobisty, datę wydania i termin ważności dowodu osobistego, podpis, nazwę organu wydającego prawo jazdy, numer prawa jazdy, kategorie prawa jazdy, datę wydania i datę ważności prawa jazdy, numer świadczenia rentowego, emerytalnego, nazwę organu wydającego legitymację ubezpieczeniową, rencisty, emeryta, datę wydania tych legitymacji,

nazwę organu wydającego książeczkę wojskową, kartę stałego lub czasowego pobytu oraz nazwę uczelni wydającej legitymację studencką - 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

Inspektor upoważniony przez Generalnego Inspektora Ochrony Danych Osobowych, przeprowadził w P. Sp. z o.o. (zwaną dalej także „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 2014 r., poz. 1182 z późn. zm.), zwaną dalej „ustawą”.

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 poprzez przetwarzanie bez podstawy prawnej danych osobowych swoich klientów (użytkowników końcowych) w następującym zakresie: kolor oczu, wzrost, wizerunek twarzy, płeć, adres zameldowania, nazwę organu wydającego dowód osobisty, datę wydania i termin ważności dowodu osobistego, podpis, nazwę organu wydającego prawo jazdy, numer prawa jazdy, kategorie prawa jazdy, datę wydania i datę ważności prawa jazdy, numer świadczenia rentowego, emerytalnego, nazwę organu wydającego legitymację ubezpieczeniową, rencisty, emeryta, datę wydania tych legitymacji, nazwę organu wydającego książeczkę wojskową, kartę stałego lub czasowego pobytu oraz nazwę uczelni wydającej legitymację studencką (art. 26 ust. 1 pkt 1 ustawy w związku z art. 161 ust. 2 ustawy Prawo telekomunikacyjne).

W związku z powyższym 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: [...]), 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.

W odpowiedzi na ww. zawiadomienie pełnomocnik Spółki pismem z dnia [...] października 2015 r. złożył w sprawie dodatkowe wyjaśnienia, z których wynika m.in., że:

1. Podstawę prawną przetwarzania danych osobowych osób, które zdecydowały się na zawarcie umowy o świadczenie usług telekomunikacyjnych, a które nie uiściły kaucji, w celu potwierdzenia

ich tożsamości, stanowi przepis art. 161 ust. 2 pkt 7 ustawy z dnia 16 lipca 2004 r. Prawo telekomunikacyjne (Dz. U. z 2014 r., poz. 243 z późn. zm.), zgodnie z którym dostawca publicznie dostępnych usług telekomunikacyjnych jest uprawniony do przetwarzania danych dotyczących użytkownika będącego osobą fizyczną zawartych w dokumentach potwierdzających możliwość wykonania zobowiązania wobec dostawcy publicznie dostępnych usług telekomunikacyjnych wynikających z umowy o świadczenie usług telekomunikacyjnych. Przepis ten w ocenie Spółki stanowi „samodzielną podstawę legalnego przetwarzania przez dostawcę usług telekomunikacyjnych szeregu danych osobowych klienta” i w związku z tym zgoda klienta (o której mowa w art. 23 ust. 1 pkt 1 ustawy) na przetwarzanie danych osobowych zawartych w kopiowanych dokumentach tożsamości nie jest niezbędna. Niemniej jednak biorąc pod uwagę fakt, iż kopie dokumentów tożsamości są niezbędne dla Spółki, jako dostawcy usług, to odmowa ich skopiowania skutkuje zawarciem umowy z dodatkowym zastrzeżeniem dotyczącym kaucji.

2. W ocenie Spółki skoro ustawodawca zezwala na uzależnienie zawarcia umowy o świadczenie usług telekomunikacyjnych od „dostarczenia” dokumentów „potwierdzających możliwość wykonania zobowiązania wobec dostawcy usług”, to tym bardziej usprawiedliwiona jest sytuacja, w której dostawca usług oczekuje kaucji od klienta, który ich nie dostarczył. Kaucja jest bowiem dodatkowym zastrzeżeniem umownym, którego celem jest „znielowanie po stronie dostawcy usług ryzyka finansowego” związanego z brakiem możliwości weryfikacji, czy klient zamierza i ma możliwość wywiązywania się ze zobowiązań na rzecz dostawcy usług. Dzięki kaucji, umowa z klientem może być zawarta pomimo braku dostatecznej, kompleksowej weryfikacji „możliwości wykonania zobowiązania wobec dostawcy usług”, jednak na odmiennych dla danego abonenta warunkach, pozwalających na ograniczenie ryzyka finansowego dostawcy usług. W związku z tym twierdzenia Generalnego Inspektora Ochrony Danych Osobowych o „presji finansowej”, jakiej rzekomo poddawany jest klient, który nie wyrazi zgody na skopiowanie dokumentów, są pozbawione słuszności.

3. Spółka chcąc zapewnić transparentność swoich działań wobec klientów, w procesie weryfikacji dokumentów przedstawianych przez klientów (podczas zawierania umowy o świadczenie usług telekomunikacyjnych), uprzedza klientów o zamiarze skopiowania dokumentów i związku z tym na tę okoliczność pozyskuje zgodę klienta (zgoda ta zamieszczona jest pod treścią umowy).

4. Zgodnie z art. 26 ust. 1 pkt 3 ustawy o ochronie danych osobowych, administrator danych powinien dołożyć szczególnej staranności w celu ochrony osób, których dane dotyczą, a w szczególności jest zobowiązany zapewnić, aby dane te były merytorycznie poprawne i adekwatne w stosunku do celów, w jakich są przetwarzane. W związku z tym Spółka przy zawieraniu z klientem umowy o świadczenie usług telekomunikacyjnych, posiada uprawnienie do przetwarzania danych osobowych zawartych w żądanych przez siebie dokumentach, w celu przeprowadzenia weryfikacji odnośnie „możliwości wykonania zobowiązania wobec dostawcy usług”.

5. Spółka zwraca również uwagę, iż nie stanowi naruszenia przepisów prawa odwoływanie się przez administratora danych jednocześnie do kilku podstaw przetwarzania danych osobowych, o których mowa w art. 23 ust. 1 ustawy o ochronie danych osobowych, w szczególności do uprawnienia administratora wynikającego z przepisu prawa (np. z art. 161 ust. 2 pkt 7 ustawy Prawo telekomunikacyjne), jak i do zgody osoby, której dane dotyczą. Na taki kierunek rozumienia relacji pomiędzy poszczególnymi przesłankami legalności przetwarzania danych osobowych wskazuje zarówno literalne brzmienie art. 23 ust. 1 ustawy o ochronie danych osobowych, który odwołuje się do: uprawnień lub obowiązków wynikających z przepisów prawa, zgody osoby, której dane dotyczą oraz do usprawiedliwionego celu przetwarzania danych przez administratora i każdą z tych przesłanek traktuje jako samodzielną i równorzędną. W związku z tym spełnienie jednej z tych przesłanek wyczerpuje wymóg legalności przetwarzania danych w konkretnym przypadku. Nie oznacza to bynajmniej, by w konkretnych okolicznościach przetwarzanie danych nie znajdowało oparcia jednocześnie w dwóch przesłankach, np. jako realizacja uprawnienia wynikającego z ustawy, a zarazem realizacja uprawnionego celu administratora danych. W związku z tym w ocenie Spółki wskazanie art. 23 ust. 1 pkt 5 ustawy o ochronie danych osobowych, jako kolejnej przesłanki legalizującej przetwarzanie danych osobowych zawartych w kserokopiach dokumentów tożsamości w sytuacji, gdy przepisy prawa telekomunikacyjnego jednoznacznie wskazują podstawy prawne przetwarzania danych w związku z zawarciem umowy o świadczenie usług telekomunikacyjnych nie prowadzi do obchodzenia prawa regulującego przedmiotowe kwestie.

6. W przypadku zawierania umowy o świadczenie usług telekomunikacyjnych za pośrednictwem internetowego kanału sprzedaży, osoba zainteresowana, zobowiązana jest do wypełnienia zamieszczonego na stronie internetowej Spółki formularza zamówienia i do zaznaczenia zawartych w tym zamówieniu oświadczeń w taki sposób, by znalazły one odzwierciedlenie na dokumencie jakim będzie umowa o świadczenie usług telekomunikacyjnych. W związku z tym wymóg złożenia przez klienta oświadczenia zawierającego jego zgodę na przetwarzanie danych zawartych w kopiach dokumentów, jest konsekwencją trybu zawarcia umowy z wykorzystaniem tego kanału sprzedaży.

7. Obecnie, w celu zapewnienia przejrzystej informacji dla osób korzystających z „internetowego kanału sprzedaży”, formularz zamówienia zamieszczony na stronie internetowej Spółki został zmodyfikowany, w ten sposób, że klient uzyskuje informację, iż w przypadku niezaznaczenia oświadczenia zawierającego zgodę na przetwarzanie danych zawartych w kopiach dokumentów, potencjalny klient ma możliwość zawarcia umowy w punkcie obsługi klienta.

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 ustawy Prawo telekomunikacyjne, 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, iż Spółka udostępnia klientom dwa kanały sprzedaży, za pośrednictwem których można zawrzeć ze Spółką umowę o świadczenie usług telekomunikacyjnych, tj.: tzw.: **kanal stacjonarny** oraz **kanal internetowy**.

Ponadto, w toku kontroli ustalono również, iż w Spółce obowiązuje dokument o nazwie „Regulamin świadczenia usług telekomunikacyjnych przez P. Sp. z o.o.[...]”, zwany dalej „regulaminem”. W § 2 regulaminu zawarte są warunki zawarcia umowy o świadczenie usług telekomunikacyjnych oraz przyczyny odmowy zawarcia takiej umowy. W pkt 1 § 2 regulaminu wskazane jest, iż <umowa zostaje zawarta z klientem, który poda aktualne dane oraz okaże ważne oryginały lub poświadczone kopie dokumentów „niezbędnych do zawarcia umowy”>. Natomiast

w § 2 pkt 2 wskazane jest, iż <Spółka ma prawo odmówić zawarcia umowy, gdy klient: „odmawia okazania lub uniemożliwia P. dokonania kopii dokumentów wymaganych przez P. w zakresie niezbędnym do zawarcia umowy lub okazane dokumenty budzą wątpliwości co do ich autentyczności” albo poda błędne lub nieaktualne dane>. W przypadku jeżeli osoba zainteresowana zawarciem umowy nie zgadza się na dokonanie kopii dokumentów, to wówczas zawarcie umowy może odbyć się jedynie na podstawie uiszczonej kaucji. W § 11 regulaminu opisane są zasady i sposoby pobierania kaucji, z których wynika m.in., iż Spółka może zażądać od klienta/abonenta przy zawieraniu umowy lub w trakcie jej trwania wpłacenia kaucji w każdym przypadku, gdy klient/abonent: odmawia okazania lub uniemożliwia Spółce dokonania kopii dokumentów wymaganych przez Spółkę w zakresie niezbędnym do zawarcia umowy lub okazane dokumenty w zakresie niezbędnym do zawarcia umowy budzą wątpliwości co do ich aktualności.

Dokonane ustalenia wykazały, iż Spółka pozyskuje od klientów, którzy zdecydowali się na zawarcie umowy o świadczenie usług telekomunikacyjnych i nie uścili kaucji, **w celu potwierdzenia ich tożsamości**, kserokopie następujących dokumentów: dowodu osobistego, legitymacji rencisty, legitymacji emeryta, legitymacji służbowej posła/senatora/nauczyciela, prawa jazdy, paszportu, legitymacji ubezpieczeniowej, książeczki wojskowej, legitymacji studenckiej, karty stałego i czasowego pobytu na terenie RP.

Z analizy treści kopii dokumentów przedstawionych w toku kontroli wynika, iż Spółka pozyskując ww. kopie zbiera dane osobowe swoich klientów, w szerszym zakresie niż zakres określony w art. 161 ust. 2 Prawa telekomunikacyjnego, tj., pozyskuje takie dane jak: kolor oczu, wzrost, wizerunek twarzy, płeć, adres zameldowania, nazwę organu wydającego dowód osobisty, datę wydania i termin ważności dowodu osobistego, podpis, nazwę organu wydającego prawo jazdy, numer prawa jazdy, kategorie prawa jazdy, datę wydania i datę ważności prawa jazdy, numer świadczenia rentowego, emerytalnego, nazwę organu wydającego legitymację ubezpieczeniową, rencisty, emeryta, datę wydania tych legitymacji, nazwę organu wydającego książeczkę wojskową, kartę stałego lub czasowego pobytu oraz nazwę uczelni wydającej legitymację studencką.

W toku kontroli ustalono również, iż przy zawieraniu umowy o świadczenie usług telekomunikacyjnych, które odbywa się **w punkcie obsługi klienta** wypełniany jest m.in. dokument o nazwie „Informacja P. Sp. z o.o. o przetwarzaniu danych osobowych oraz oświadczenia klienta/abonenta” (dokument ten stanowi załącznik nr [...] do umowy). W pkt 6 przedmiotowego dokumentu zawarta jest m.in. następująca informacja: *wyrażam zgodę na podstawie art. 161 ust. 3 ustawy prawo telekomunikacyjne na przetwarzanie danych wskazanych na pierwszej stronie umowy w polach oznaczonych indeksem 1 w brzmieniu „pole wypełnione za zgodą abonenta” a także danych zawartych w kopiach dokumentów przedstawionych przy zawieraniu umowy, danych karty kredytowej, adres e-mail, kontaktowego numeru telefonu.*

Ponadto ustalono, iż w przypadku zawierania umowy o świadczenie usług telekomunikacyjnych za pośrednictwem **internetowego kanału sprzedaży**, klient w formularzu o nazwie „Oświadczenia” obowiązkowo musi zaznaczyć jedno z pól oznaczonych gwiazdką. W polu tym wśród innych oświadczeń zawarta jest klauzula następującej treści „*wyrażam zgodę (na podstawie art. 161 ust 3 ustawy z dnia 16 lipca 2004 r. Prawa telekomunikacyjnego (...)) na przetwarzanie danych wskazanych na pierwszej stronie umowy w polach oznaczonych indeksem 1 w brzmieniu „pole wypełnione za zgodą abonenta” a także danych zawartych w kopiach dokumentów przedstawionych przy zawieraniu umowy, danych karty kredytowej, adres e-mail, kontaktowego numeru telefonu podanych trakcie trwania umowy a) w celu podjęcia działań przed zawarciem umowy, b) w celu realizacji umowy, do wypełnienia prawnie usprawiedliwionych celów P. Sp. z o.o. w tym sprzedaży i marketingu bezpośredniego, własnych produktów i usług, c) dochodzenia roszczeń z tytułu prowadzonej działalności gospodarczej oraz pozostałych celach statutowych, d) gdy jest niezbędne do zrealizowania uprawnienia lub spełnienia obowiązku wynikającego przepisu prawa lub do wykonania określonych prawem zadań realizowanych dla dobra publicznego. Zgoda na przetwarzanie ww. danych w celach marketingowych jest niezależna od czasu obowiązywania umowy*”. Jak wynika z ww. formularza pole zawierające przedmiotową klauzulę opatrzone jest gwiazdką (jako oświadczenie wymagane). W związku z tym uznać należy, iż osoba wypełniająca przedmiotowy formularz nie może odmówić wyrażenia zgody na przetwarzanie danych osobowych zawartych w kopiowanych dokumentach tożsamości.

W toku kontroli ustalono również, iż w zawartych już umowach o świadczenie usług telekomunikacyjnych na ostatniej stronie (nad miejscem przeznaczonym na złożenie podpisu przez strony zawartej umowy), zamieszczone są oświadczenia o następującej treści: „*1) oświadczam, iż otrzymałam/em i akceptuję regulamin wybranej promocji określonej na stronie 1 umowy (nie dotyczy umów zawieranych poza promocją); 2) oświadczam, że zapoznałam/em się z zakresem usług, postanowieniami i warunkami umowy, a także że otrzymałam/łem i akceptuję Regulamin świadczenia usług telekomunikacyjnych przez P. Sp. z o.o.- abonament, cennik stanowiący integralną część umowy, w szczególności postanowienia o odpowiedzialności P. Sp. z o.o. za niewykonanie i nienależyte wykonanie umowy, postanowienia dotyczące zasad rozwiązywania umowy oraz postanowienia dotyczące zasad naliczania kar umownych i ich wysokości; 3) oświadczam, że wyrażam zgodę na wykonanie kopii dokumentów przedstawionych przy zawarciu umowy, a tym samym na przetwarzanie danych w nich zawartych w celach zawarcia umowy i archiwizacji; 4) abonent prowadzący działalność gospodarczą oświadcza, że w dniu zawierania umowy prowadzi działalność gospodarczą i potwierdza, że dane podane na 1 stronie umowy są aktualne*”. W związku z tym uznać należy, iż osoba podpisująca umowę o świadczenie usług telekomunikacyjnych również nie może odmówić wyrażenia zgody na przetwarzanie danych

osobowych zawartych w kopiowanych dokumentach tożsamości, a tym samym na przetwarzanie danych w nich zawartych w celach zawarcia umowy.

W piśmie (znak: [...]) stanowiącym odpowiedź na zawiadomienie o wszczęciu postępowania administracyjnego, pełnomocnik Spółki wskazał, iż podstawę prawną przetwarzania danych osobowych osób, które zdecydowały się na zawarcie umowy o świadczenie usług telekomunikacyjnych, a które nie uiściły kaucji, **w celu potwierdzenia ich tożsamości** stanowi przepis art. 161 ust. 2 pkt 7 ustawy z dnia 16 lipca 2004 r. Prawo telekomunikacyjne (Dz. U. z 2014 r., poz. 243 z późn. zm.), zgodnie z którym dostawca publicznie dostępnych usług telekomunikacyjnych jest uprawniony 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. Przepis ten w ocenie Spółki stanowi „samodzielną podstawę legalnego przetwarzania przez dostawcę usług telekomunikacyjnych szeregu danych osobowych klienta”.

Nie można zgodzić się z tą argumentacją Spółki, bowiem zauważyć należy, iż kwestia zakresu danych pozyskiwanych, w związku z **identyfikacją użytkownika końcowego 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.

W ocenie Generalnego Inspektora Ochrony Danych Osobowych treść art. 161 ust. 2 pkt 7 ww. ustawy powinna być rozumiana 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 końcowego, również danych zawartych w dokumentach służących ustaleniu, czy użytkownik końcowy będzie w stanie wykonać zobowiązanie względem dostawcy publicznie dostępnych usług telekomunikacyjnych. W związku z tym, że zobowiązanie użytkownika końcowego polega na zapłacie należności pieniężnej, dostawca usług może pozyskiwać kopie dokumentów potwierdzających zdolność do wykonania zobowiązania pieniężnego i przetwarzać dane zawarte w tych dokumentach.

W tym miejscu należy podkreślić, iż dane osobowe zawarte w kopiowanym dokumencie jakim jest dowód osobisty potwierdzają tożsamość i obywatelstwo danej osoby. Natomiast dane osobowe zawarte w kopiowanych dokumentach takich jak: prawo jazdy, legitymacja ubezpieczeniowa rencisty, emeryta, książeczka wojskowa, karta stałego lub czasowego pobytu oraz legitymacja studencka potwierdzają tożsamość danej osoby oraz jej uprawnienia. A zatem stwierdzić należy, iż ww. dokumenty nie zawierają informacji, na podstawie których można dokonać oceny czy użytkownik końcowy będzie w stanie wykonać zobowiązanie pieniężne względem dostawcy publicznie dostępnych usług telekomunikacyjnych.

Należy w tym miejscu zaznaczyć, że z materiału dowodowego zebranego w toku niniejszego postępowania administracyjnego, w tym z wyjaśnień pozyskanych w toku kontroli wynika jednoznacznie, że kwestionowane dane osobowe nie są zbierane przez Spółkę w celu potwierdzenia zdolności do wykonania zobowiązania pieniężnego przez użytkownika końcowego, ale **wyłącznie w celu identyfikacji jego tożsamości.**

Poza tym, Generalny Inspektor Ochrony Danych Osobowych podejmując niniejsze rozstrzygnięcie nie odnosi się do kwestii, czy którakolwiek z danych osobowych, których przetwarzanie przez Spółkę jest przedmiotem niniejszego postępowania mogłaby potwierdzać zdolność do wykonania zobowiązania pieniężnego przez klienta, lecz ocenia kwestię, czy Spółka posiada podstawę prawną do przetwarzania danych osobowych w zakresie wykraczającym poza zakres wskazany w art. 161 ust. 2 ustawy Prawo telekomunikacyjne **w celu identyfikacji klienta (użytkownika końcowego).**

Wobec powyższego Generalny Inspektor Ochrony Danych Osobowych uznał, iż art. 161 ust. 2 pkt 7 ustawy Prawo telekomunikacyjne nie stanowi podstawy prawnej do przetwarzania kwestionowanych danych osobowych **w celu prawidłowej identyfikacji użytkownika końcowego.**

Ponadto, należy nadmienić, iż konsekwencją przyjęcia interpretacji art. 161 ust. 2 pkt 7 ustawy Prawo telekomunikacyjne proponowanej przez pełnomocnika Spółki, zgodnie z którą ww. przepis uprawnia dostawcę usług do przetwarzania danych zawartych w dokumentach, byłoby pozbawienie znaczenia unormowania zawartego w art. 161 ust. 2 pkt 1-6 ustawy Prawo telekomunikacyjne, które tworzy zamknięty katalog danych, na podstawie których można dokonać **identyfikacji użytkownika końcowego**, do przetwarzania których uprawniony jest dostawca publicznie dostępnych usług telekomunikacyjnych.

Również nie można zgodzić się z argumentacją Spółki, iż podstawę prawną przetwarzania kwestionowanych danych osobowych stanowi art. 23 ust. 1 pkt 5 oraz art. 26 ust. 1 pkt 3 ustawy, o ochronie danych osobowychalbowiem powoływanie ww. przepisów ustawy, jako kolejnych przesłanek legalizujących przetwarzanie danych osobowych zawartych w kserokopiach dokumentów tożsamości w sytuacji, gdy przepisy prawa telekomunikacyjnego jednoznacznie wskazują podstawy prawne przetwarzania danych w związku z zawarciem umowy o świadczenie usług telekomunikacyjnych, prowadzi niewątpliwie do obchodzenia prawa regulującego przedmiotowe kwestie.

Za podstawę prawną przetwarzania kwestionowanych danych nie można również przyjąć zgody na przetwarzanie danych osobowych, o której mowa w art. 23 ust 1 pkt 1 ustawy. Należy bowiem wskazać, iż na podstawie analizy zapisów umieszczonych w zawartych umowach o świadczeniu usług telekomunikacyjnych, jak również informacji zawartych w formularzu o nazwie „Oświadczenie” (wypełnianym przy zawieraniu umowy przez Internet), Spółka jako

administrator danych zamieściła wśród innych oświadczeń woli klauzulę *zgody na dokonanie kserokopii dokumentów przedstawionych przy zawarciu umowy o świadczenie usług telekomunikacyjnych, a tym samym na przetwarzanie danych w nich zawartych*, co w ocenie Generalnego Inspektora Ochrony Danych Osobowych narusza art. 174 pkt 1 ustawy Prawo telekomunikacyjne, zgodnie z którym zgoda na przetwarzanie danych osobowych nie może być domniemana lub dorozumiana z oświadczeniem woli o innej treści.

W związku z tym decyzja w sprawie wyrażenia zgody na przetwarzanie danych osobowych powinna być podjęta swobodnie i mieć charakter samodzielny. Należy bowiem tu wskazać, że istotą przesłanki zgody jest oparcie jej na dobrowolnym oświadczeniu osoby, której dane dotyczą, wyrażającym przyzwolenie na przetwarzanie dotyczących jej danych osobowych, a brak swobody w zakresie wyrażenia zgody na przetwarzanie danych osobowych prowadzi do ograniczenia praw osób fizycznych przejawiających się m.in. w prawie do dysponowania swoimi danymi osobowymi. Warto w tym miejscu wskazać również, że wytyczne dotyczące sposobu pozyskiwania zgody abonenta lub użytkownika końcowego zawarte w ustawie Prawo telekomunikacyjne są wynikiem definicji zawartej w art. 2 lit. f dyrektywy 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. dotyczącej przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (dyrektywa o prywatności i łączności elektronicznej) (Dz. Urz. WE L 201 z 31.07.2002, s. 37), która w sprawie zgody udzielanej przez użytkownika lub abonenta odsyła do zgody podmiotu danych w rozumieniu dyrektywy 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych (Dz. Urz. WE L 281 z 23.11.1995, s. 31) stanowiąc, iż: „zgoda użytkownika lub abonenta odpowiada zgodzie podmiotu danych określonej w dyrektywie 95/46/WE”.

W związku z powyższym w każdym przypadku, gdy na mocy dyrektywy o prywatności i łączności elektronicznej wymagana jest zgoda, kryteria służące ustaleniu, czy zgoda jest ważna są takie same, jak określone w dyrektywie 95/46/WE, tj. zgodne z definicją zawartą w art. 2 lit. h oraz warunkami określonymi w art. 7 lit. a. Zgodnie zaś z art. 2 lit. h dyrektywy 95/46/WE *zgoda osoby, której dane dotyczą* oznacza konkretne i świadome, dobrowolne wskazanie przez osobę, której dane dotyczą na to, że wyraża przyzwolenie na przetwarzanie odnoszących się do niej danych osobowych". Szczególny charakter przesłanki zgody z punktu widzenia autonomii informacyjnej osoby, której dane dotyczą, został podkreślony w opinii Grupy Roboczej ds. Ochrony Osób Fizycznych w zakresie Przetwarzania Danych Osobowych powołanej na mocy art. 29 dyrektywy 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych - nr 15/2011 *W sprawie definicji zgody* (strona 9 - pkt 11.3. *Pojęcia powiązane*), w której wskazano iż: „Kontrola sprawowana poprzez zgodę jest ważnym pojęciem z punktu widzenia praw podstawowych. Jednocześnie - i z tego samego punktu

widzenia - decyzja osoby fizycznej o zgodzie na czynność przetwarzania danych powinna podlegać rygorystycznym wymogom, zwłaszcza biorąc pod uwagę fakt, że podejmując taką decyzję, osoba ta może zrzekać się prawa podstawowego. (...) Zgoda wiąże się z koncepcją informacyjnego samostanowienia. Autonomia osoby, której dane dotyczą, jest zarówno warunkiem wstępnym, jak i konsekwencją zgody: umożliwia ona tej osobie wywieranie wpływu na przetwarzanie danych osobowych".

W związku z powyższym na podstawie materiału dowodowego zgromadzonego w niniejszej sprawie stwierdzić należy, że Spółka zarówno w procesie zawierania umowy o świadczenie usług telekomunikacyjnych, które odbywa się **w punktach obsługi klienta** oraz za pośrednictwem kurierów **(w przypadku internetowego kanału sprzedaży)** - nie zapewniła swobody w zakresie wyrażenia zgody na przetwarzanie danych osobowych zawartych w kserokopiach dokumentów przedstawionych przy zawarciu umowy o świadczenie usług telekomunikacyjnych i tym samym naruszyła art. 174 pkt 1 ustawy Prawo telekomunikacyjne.

Odnosząc się natomiast do wyjaśnień Spółki, iż zawarcie umowy o świadczenie usług telekomunikacyjnych musi być poprzedzone potwierdzeniem tożsamości osoby zawierającej ze Spółką umowę, wskazać należy, iż Generalny Inspektor Ochrony Danych Osobowych nie kwestionuje tego, iż Spółka jako operator telekomunikacyjny, w celu zawarcia umowy o świadczenie usług telekomunikacyjnych jest zobowiązana potwierdzić tożsamość klienta (tj. użytkownika końcowego), z którym ma być zawarta umowa. W tym celu Spółka ma prawo przetwarzać dane osobowe wskazane w art. 162 ust. 2 pkt 1-6 ustawy Prawo telekomunikacyjne, natomiast inne dane Spółka może przetwarzać na podstawie art. 161 ust. 3 ustawy Prawo telekomunikacyjne tj. za zgodą, osoby, której dane dotyczą, pod warunkiem, iż zgoda ta będzie spełniała wymogi określone art. 174 pkt 1 ustawy Prawo telekomunikacyjne, zgodnie z którym zgoda na przetwarzanie danych osobowych nie będzie domniemana lub dorozumiana z oświadczenia woli o innej treści.

Należy też jednoznacznie wskazać, iż w ocenie Generalnego Inspektora Ochrony Danych Osobowych dopuszczalne jest również to, iż w celu prawidłowej identyfikacji klienta Spółka może sporządzać kserokopie dokumentów potwierdzających jego tożsamość, ale jedynie pod warunkiem anonimizacji danych osobowych, do przetwarzania których Spółka nie jest uprawniona.

Generalny Inspektor nie kwestionuje również tego, iż w przypadku kiedy osoba zainteresowana zawarciem umowy odmawia okazania dokumentu służącego do ustalenia jej tożsamości, lub nie wyrazi zgody na skopiowanie takiego dokumentu (pod warunkiem anonimizacji danych do przetwarzania których Spółka nie jest uprawniona), to w takim przypadku zawarcie umowy możliwe jest po przyjęciu zabezpieczenia w postaci kaucji.

Jednocześnie odnosząc się do wyjaśnień pełnomocnika Spółki zawartych w odpowiedzi na zawiadomienie o wszczęciu postępowania administracyjnego, z których wynika, iż „obecnie w celu zapewnienia przejrzystej informacji dla osób korzystających z internetowego kanału sprzedaży formularz zamówienia został zmodyfikowany, w ten sposób, że klient uzyskuje informację, iż w przypadku niezaznaczenia oświadczenia zawierającego zgodę na przetwarzanie danych zawartych w kopiach dokumentów, potencjalny klient ma możliwość zawarcia umowy w punkcie obsługi klienta”, należy wskazać, iż do dnia wydania niniejszej decyzji Spółka nie przedstawiła dowodów potwierdzających złożone wyjaśnienia. Ponadto, brak jest informacji, czy zostały zmodyfikowane w Spółce procedury dotyczące zawarcia umowy o świadczenie usług telekomunikacyjnych (tj. procedury dotyczące zawierania umowy w punkcie obsługi klienta, jak i procedury dotyczące zawierania umowy z wykorzystaniem internetowego kanału sprzedaży).

Z tych też względów w ocenie Generalnego Inspektora Ochrony Danych Osobowych zarzut braku swobody w kwestii wyrażenia zgody przez osoby wypełniające formularz zamówienia, zamieszczony na stronie internetowej nie mógłby zostać uznany za usunięty poprzez przekazanie ww. osobom informacji o treści zacytowanej powyżej. Bowiernie takie działanie Spółki należałoby uznać za działanie pozorne i niekorzystne dla osób zainteresowanych zawarciem umowy o świadczenie usług telekomunikacyjnych za pośrednictwem kanału internetowego, bowiem pozbawiałoby możliwości skorzystania ze zdalnego kanału sprzedaży i wymuszałoby konieczność osobistego zgłoszenia się do punktu obsługi klienta, w celu przekazania kopii dokumentu służącego do potwierdzenia tożsamości, co w konsekwencji prowadziłoby do przetwarzania w dalszym ciągu danych osobowych wykraczających poza zakres wskazany w art. 161 ust. 2 ustawy Prawo telekomunikacyjne, do przetwarzania których Spółka nie jest uprawniona.

Wobec powyższych ustaleń, Generalny Inspektor uznał, iż Spółka nie legitymuje się zgodą na przetwarzanie danych osobowych innych niż wskazane w art. 161 ust. 2 ustawy Prawo telekomunikacyjne (tj. takich jak: kolor oczu, wzrost, wizerunek twarzy, płeć, adres zameldowania, nazwę organu wydającego dowód osobisty, datę wydania i termin ważności dowodu osobistego, podpis, nazwę organu wydającego prawo jazdy, numer prawa jazdy, kategorie prawa jazdy, datę wydania i datę ważności prawa jazdy, numer świadczenia rentowego, emerytalnego, nazwę organu wydającego legitymację ubezpieczeniową, rencisty, emeryta, datę wydania tych legitymacji, nazwę organu wydającego książeczkę wojskową, kartę stałego lub czasowego pobytu oraz nazwę uczelni wydającej legitymację studencką), a ponadto żadna inna przesłanka przetwarzania ww. danych nie ma w niniejszej sprawie zastosowania.

Dlatego też Spółka przetwarzając kwestionowane dane osobowe narusza tym samym przepis art. 161 ust. 3 w związku z art. 174 ustawy Prawo telekomunikacyjne.

Mając powyższe na uwadze, w tym stanie faktycznym i prawnym, 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 2014 r., poz. 1619 z późn. zm.).