Ewa Kulesza

Ochrona danych osobowych klientów jako element działania etycznego przedsiębiorcy

Annales. Etyka w życiu gospodarczym 13/1, 97-105

2010

Ewa Kulesza
Uniwersytet Łódzki
Salezjańska Wyższa Szkoła Ekonomii i Zarządzania, Łódź

Ochrona danych osobowych klientów jako element działania etycznego przedsiębiorcy

Prawo do prywatności i stanowiące jego element, wyodrębnione nieco później, prawo do ochrony danych osobowych, należą do podstawowych praw człowieka. Ich znaczenie podkreślają fundamentalne dla nas normy prawa międzynarodowego, jak Europejska Konwencja Praw Człowieka i Podstawowych Wolności, prawa europejskiego – w tym Karta Praw Podstawowych Unii Europejskiej, a także ustawodawstwo krajowe.

Ze względu na istotę prawa do prywatności i ochrony danych osobowych, regulujące je normy prawa nabierają szczególnego znaczenia, nie są bowiem jedynie instrumentem ochrony określonych interesów państwa, ale instrumentem ochrony praw człowieka.

1. Uchwalona w sierpniu 1997 r. ustawa o ochronie danych osobowych[1] nałożyła na wszystkie podmioty wykorzystujące w swojej działalności zawodowej dane osobowe, określone obowiązki związane z ich ochroną oraz zagwarantowała osobom, których dane są przetwarzane, uprawnienia mające zapewnić kontrolę przetwarzania tych danych.

Przyjęcie do polskiego ustawodawstwa ustawy o ochronie danych osobowych stanowiło przeniesienie do polskiego systemu prawnego filozofii i zasad ochrony danych osobowych szczegółowo określonych w Dyrektywie 95/46[2]. Było także wykonaniem wynikających z umów akcesyjnych zobowiązań Polski do dostosowania ustawodawstwa do norm Unii Europejskiej, a także realizacją konstytucyjnej normy gwarantującej prawo do ochrony danych osobowych.

Dyrektywa zawiera wyraźne podkreślenie, iż integracja ekonomiczno-społeczna musi prowadzić do znacznego zwiększenia przepływu danych osobowych pomiędzy wszystkimi podmiotami zaangażowanymi prywatnie lub publicznie w działalność ekonomiczną i społeczną, a integracja polityczna, do wymiany pomiędzy władzami poszczególnych państw – na podstawie prawa Wspólnoty – danych osobowych, w celu wykonywania obowiązków oraz realizacji zadań określonych przepisami prawa. Jednakże, co wynika również z Dyrektywy, warunkiem swobodnej wymiany danych musi być zagwarantowanie każdej jednostce praw podstawowych: prywatności i ochrony danych osobowych. Oznacza to, iż wymiana danych musi odbywać się z zapewnieniem poufności oraz z zabezpieczeniem danych przed nielegalnym przetwarzaniem, nieuprawnionym udostępnieniem, zmianą czy utratą, jak też gwarantować osobom, których dane dotyczą (podmiotom danych) podstawowe uprawnienia stanowiące istotę ochrony danych: prawo do informacji i prawo do kontroli przetwarza-

[1] Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r., Nr 101, poz. 926 ze zm.).

[2] Dyrektywa Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych oraz swobodnego przepływu tych danych.

nia danych. Brak owych gwarancji praw podstawowych, bądź różnice w stopniu ochrony prywatności i danych osobowych w różnych państwach, mogłyby doprowadzić do ograniczania wymiany danych ze względu na różnice w stopniu ochrony praw i swobód jednostek, a nawet uniemożliwić szereg przedsięwzięć ekonomicznych, czy utrudniać władzom publicznym wykonywanie wynikających z przepisów prawa obowiązków. Z tego też względu stopień ochrony praw i swobód jednostek w zakresie prywatności i ochrony danych osobowych musi być równoważny we wszystkich państwach prowadzących wspólny rynek i współdziałających w zakresie wykonywania określonych działań politycznych i społecznych.

W Dyrektywie zostały zatem wskazane dwa podstawowe filary współpracy gospodarczej i politycznej: dopuszczalność, a nawet konieczność wymiany danych osobowych we współpracy pomiędzy państwami, zwłaszcza w obrocie gospodarczym, zaś drugiej strony – obowiązek ochrony danych i zagwarantowanie określonych praw osobom, których dane są przetwarzane (wykorzystywane) przez podmioty publiczne i prywatne (administratorów danych).

Wśród obowiązków w zakresie ochrony danych osobowych spoczywających na administratorach danych, obok przetwarzania jedynie na podstawie legalnych przesłanek i odpowiedniego zabezpieczenia danych, Dyrektywa nakazuje zagwarantowanie osobom, których dane dotyczą, prawa do informacji o przetwarzaniu danych oraz prawa dostępu i weryfikacji dotyczących ich danych. Obowiązkom administratorów danych odpowiadają prawa osób, których dane dotyczą, w tym fundamentalne prawa do informacji, do sprzeciwu przeciwko przetwarzaniu ich danych, czy do poprawy, usunięcia lub zablokowania danych, których przetwarzanie jest niezgodne z postanowieniami Dyrektywy *w szczególności ze względu na ich niekompletność lub niedokładność*.

Te elementy prawa do ochrony danych osobowych akcentuje również Konstytucja RP, gwarantująca każdemu w art. 51 prawo do „ informacyjnego samookreślenia". Art. 51 Konstytucji stanowi, iż każda osoba – nie tylko obywatel – przebywająca na terytorium RP zobowiązana jest do udostępniania danych jedynie na podstawie ustawy oraz że każdemu przysługuje prawo dostępu do dotyczących go urzędowych dokumentów i zbiorów danych, a także prawo do sprostowania oraz usunięcia informacji nieprawdziwych, niepełnych lub zebranych w sposób sprzeczny z ustawą.

2. Ustawa o ochronie danych osobowych, będąca realizacją postanowień Dyrektywy i art. 51 Konstytucji RP[3], nie ograniczając możliwości wykorzystywania danych, zarówno w działalności podmiotów publicznych, jak i podmiotów należących do sektora prywatnego, nałożyła na nie określone obowiązki. Zgodnie z przepisami ustawy, każdy podmiot zbierający, utrwalający, przechowujący, zmieniający, czy usuwający, tzn. przetwarzający[4] dane osobowe jest tzw. administratorem danych[5], zobowiązanym do dołożenia szczególnej staranności w celu ochrony interesów osób, których dane dotyczą. Według art. 26 ust. 1 ustawy owo dołożenie szczególnej staranności winno polegać zwłaszcza na zapewnieniu, aby

[3] Art. 51 ust. 5 Konstytucji stanowiąc, iż *zasady i tryb gromadzenia oraz udostępniania informacji określa ustawa*, zapowiedział uchwalenie odrębnej ustawy określającej wszystkie szczegółowe kwestie związane z realizacją, ogólnie sformułowanego w Konstytucji, prawa do ochrony danych osobowych.

[4] Pojęcie „przetwarzania" zdefiniowane zostało w art. 7 pkt. 2 ustawy o ochronie danych osobowych i rozumie się przez nie *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*.

[5] Definicja administratora danych podana została w art. 7 pkt. 4 ustawy o ochronie danych osobowych.

dane były przetwarzane zgodnie z prawem, zbierane dla oznaczonych, zgodnych z prawem celów i nie poddawane dalszemu przetwarzaniu niezgodnemu z tymi celami, a także merytorycznie poprawne i adekwatne do celów przetwarzania oraz przechowywane w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej, niż jest to niezbędne do osiągnięcia celu przetwarzania. Zasady, o których mowa w art. 26 ustawy o ochronie danych, mają szczególne znaczenie dla administratorów z sektora prywatnego (przedsiębiorców). W tym przypadku bowiem podstawą gromadzenia danych nie jest – jak w przypadku organów państwa – przepis prawa, ale inna z przesłanek wskazanych w art. 23 ustawy o ochronie danych osobowych, określającym zgodne z prawem podstawy przetwarzania. W przypadku podmiotów sektora prywatnego taką podstawą może być np. umowa pomiędzy przedsiębiorcą a osobą, której dane dotyczą, czy zgoda takiej osoby na wykorzystywanie jej danych w celach marketingowych.

Ustawodawca, podkreślając obowiązek dołożenia przez administratora danych szczególnej staranności w ochronie interesów osób, których dane dotyczą i wskazując, iż dane mają być przetwarzane zgodnie z prawem, stawia wymóg przestrzegania zasad określonych w ustawie o ochronie danych osobowych. Oznacza to, że gromadzenie i wykorzystywanie danych winno odbywać się wyłącznie na podstawie jednej z przesłanek wymienionych w art. 23 ust. 1 lub art. 27 ust. 2 ustawy o ochronie danych, dla oznaczonych, zgodnych z prawem celów i że dane nie mogą być przetwarzane w sposób niezgodny z tymi celami oraz że administrator danych jest zobowiązany wykonywać wskazane w ustawie obowiązki, zarówno w zakresie zabezpieczenia danych, jak i też obowiązki gwarantujące prawa osób, których dane wykorzystuje, szczegółowo opisane w przepisach o ochronie danych osobowych. W tym zakresie, polska ustawa o ochronie danych osobowych, analogicznie jak Dyrektywa UE, podkreślając możliwość wykorzystania danych osobowych, stawia administratorom danych określone wymogi, w tym warunek zagwarantowania osobom, których dane dotyczą, przysługujących im praw. Oznacza to, że ochrona danych osobowych nie uniemożliwia wykorzystywania danych osobowych do prowadzenia działalności gospodarczej, nakazuje jednak, aby każdy podmiot przetwarzający dane osobowe, a zatem m.in. zbierający, utrwalający, przechowujący, opracowujący, zmieniający, czy udostępniający dane osobowe, działał zgodnie z przepisami ustawy o ochronie danych oraz z zasadami w niej określonymi, nie naruszając praw osób, których dane wykorzystuje.

Należy podkreślić, iż przepisy z zakresu ochrony danych osobowych nie określają jedynie abstrakcyjnych i uciążliwych dla administratora danych obowiązków. Ich wykonanie przez administratora danych ma nie tylko zagwarantować bezpieczeństwo danych, odpowiedniość (adekwatność danych) do celu ich gromadzenia i wykorzystywania, ale także umożliwić osobie, której dane dotyczą, kontrolę przetwarzania danych, w tym prawo do ich poprawiania, czy aktualizacji w przypadku ich niekompletności, braku aktualności zbędności dla realizacji określonego celu bądź zebrania z naruszeniem prawa. Jest bowiem kwestią niezwykle istotną, aby podmiot zbierający i wykorzystujący dane nie tylko przetwarzał je wyłącznie w zakresie niezbędnym dla realizacji celów, ale dawał gwarancję, że nie zostaną one wbrew woli osoby lub poza jej świadomością, wykorzystane w innym celu, lub przez inny podmiot, bądź że dane te nie będą prawdziwe bądź aktualne. Owo nie wykorzystywanie danych w innym celu niż cel przetwarzania ma być zagwarantowane również poprzez nakazanie przechowywania w postaci umożliwiającej identyfikację jedynie do momentu realizacji celu.

3. Wykonanie obowiązków z ustawy o ochronie danych osobowych nabiera szczególnego znaczenia w przypadku przetwarzania danych, czyli ich gromadzenia i wykorzysty-

wania przez podmioty sektora prywatnego. O ile bowiem podmioty publiczne mają konstytucyjny obowiązek działania na podstawie i w granicach prawa, co oznacza, że to ustawodawca przesądza zarówno o zakresie, jak i celu przetwarzania danych przez te pomioty, to administratorzy należący do sektora prywatnego przede wszystkim uzyskują dane w ramach zawieranych umów bądź opierają się na zgodzie klientów na przetwarzanie danych, opartej często na zaufaniu do podmiotu żądającego danych. Z tego względu zgoda musi być świadomym wyrażeniem woli, udzielonym po uzyskaniu podstawowych, rzetelnie przedstawionych informacji dotyczących przetwarzania.

Z tego względu wyjątkowo ważne jest wykonanie przez podmiot żądający danych obowiązku informacyjnego wobec osoby, od której żąda danych lub której dane uzyskane zostały od innego podmiotu. Pozwala bowiem osobie, której dane dotyczą, na podjęcie świadomej decyzji o ich udostępnieniu, bądź umożliwia skorzystanie z przysługujących jej uprawnień, gdy administrator danych uzyskał je od innego podmiotu. Ważne jest zwłaszcza udzielenie informacji o samym przyszłym administratorze danych, celu przetwarzania, którego doprecyzowanie może przesądzić o wyrażeniu zgody na udostępnienie i przetwarzanie danych, bądź nie oraz o obowiązku lub dobrowolności udostępnienia danych.

Udzielenie informacji o samym administratorze danych nie może ograniczyć się do podania samej nazwy firmy, bądź nazwy z adresem skrytki pocztowej, ale musi obejmować całą nazwę firmy, a także jej dokładny adres, co pozwoli na skontaktowanie się osoby, której dane są wykorzystywane z podmiotem gospodarczym w sytuacji, gdyby osoba ta chciała skontrolować, jak w rzeczywistości jej dane są wykorzystywane, bądź w celu realizacji przysługujących jej praw, w tym prawa do sprzeciwu wobec wykorzystywania jej danych bądź żądania usunięcia danych. Obowiązek informacyjny powinien obejmować także określenie celu gromadzenia danych oraz określenie podmiotów będących odbiorcami danych, albo przynajmniej kategorii takich podmiotów. Wreszcie, obowiązek informacyjny powinien wskazywać na prawo dostępu do treści danych oraz na prawo ich poprawiania, jak też prawo do zażądania usunięcia danych bądź nie wykorzystywania danych w celach marketingowych.

4. Omówione powyżej obowiązki administratorów danych osobowych, wynikające z ustawy o ochronie danych osobowych, postrzegać należy nie tylko przez pryzmat wykonywania obowiązujących przepisów, ale także jako gwarancje prawa do prywatności i ochrony danych osób, których dane administrator przetwarza, zapewniające bezpieczeństwo danych powierzonych podmiotowi (administratorowi danych) przez osobę w określonym celu i adekwatnych (odpowiednich) do celu przetwarzania.

Ustawa wymaga, co zostało podkreślone w niniejszym tekście, iż administrator danych jest zobowiązany do szczegółowego informowania o celu gromadzenia danych oraz o obowiązku lub dobrowolności przekazania – gromadzenia danych osobowych, bowiem od jego wiedzy zależy, czy wyrazi zgodę na przetwarzanie danych. Administrator powinien poinformować również o ewentualnym przekazywaniu danych innym podmiotom, ze wskazaniem przynajmniej kategorii podmiotów, którym dane byłyby przekazywane. Dopiero całościowa wiedza o celu przetwarzania, obowiązku lub dobrowolności udostępniania danych, ewentualnej możliwości przekazywania danych innym podmiotom, przysługujących prawach, pozwala osobie na świadome wyrażenie zgody na przetwarzanie. Podanie powyższych informacji jest jednak równie ważne dla osoby, której dane są gromadzone, jak i dla administratora danych (przedsiębiorcy), który może wykorzystywać dane w takich granicach, o jakich informował osobę dane udostępniającą. Można stwierdzić, że wykona-

nie obowiązku informacyjnego jest w równym stopniu ważne i wiążące dla samej osoby udostępniającej dane, jak dla administratora danych (przedsiębiorcy).

Tymczasem powszechną praktyką przedsiębiorców jest niedopełnienie obowiązku informacyjnego poprzez niepodanie celu przetwarzania danych, wprowadzenie w błąd przez podanie innego celu, niż rzeczywisty, bądź podanie niekompletnych danych, potem zaś dowolne wykorzystywanie danych klientów. W wielu przypadkach, zwłaszcza firmy marketingowe, unikały przekazywania klientom informacji o źródle pozyskania danych, bądź informacji o pełnej nazwie i adresie siedziby firmy, co uniemożliwiało skorzystanie przez klientów z przysługujących im praw, np. prawa do złożenia sprzeciwu co do dalszego wykorzystywania ich danych dla celów marketingowych[6]. Natomiast, nawet jeśli podana była informacja identyfikująca firmę (np. firmę marketingową), osoby do których kierowana była przesyłka nie mogły skutecznie skorzystać z prawa złożenia sprzeciwu wobec przetwarzania ich danych – składane sprzeciwy nie były respektowane przez firmę bądź były uwzględniane dopiero po interwencji organu ochrony danych osobowych.

Naruszenie uprawnień klientów polegało również na braku możliwości nie wyrażenia zgody na wykorzystanie danych w różnych celach (np. w celu przekazywania danych tzw. "podmiotom współpracującym") w związku z takim sformułowaniem formularza, który nie przewiduje możliwości wyboru; brak sprzeciwu na dowolne wykorzystanie danych – wobec braku możliwości nie wyrażenia zgody klientów – stanowił pretekst do dowolnego wykorzystywania, a nawet sprzedawania danych innym podmiotom[7].

Ze zbiorów danych, przetwarzanych na potrzeby zawarcia umowy, tworzone były podzbiory, sprzedawane innym podmiotom gospodarczym, najczęściej firmom marketingowym, a wielość dodatkowych informacji o kliencie ułatwiała tworzenie takich podzbiorów według różnych kryteriów (np. wieku, miejsca zamieszkania, wykształcenia). Administrator danych uznawał, że skoro przetwarza dane na podstawie zgody klienta, to staje się „właścicielem" danych, a zatem może je używać w sposób dowolny, niezależnie od celu gromadzenia danych, o którym informował klienta. Uznawał także, że może traktować zbiór jako dodatkowe źródło zysków ze sprzedaży danych. A że nie jest to przykład hipotetycznego, nagannego działania administratora danych, świadczyć może wyrok NSA z lutego 2008 r. zakazujący jednemu z operatorów sieci telefonicznej sprzedaży, tworzonych ze zbioru klientów, podzbiorów oferowanych odpłatnie innym firmom[8].

Naruszeniem ustawy o ochronie danych osobowych, ale również naruszeniem prywatności klientów jest gromadzenie przez przedsiębiorcę – pod groźbą nie zawarcia umowy – wielu szczegółowych, zbędnych informacji dotyczących klienta. Klasycznym przykładem w tym zakresie było żądanie niegdyś przez przedstawicieli operatorów sieci telefonicznych dwóch, a nawet trzech dokumentów potwierdzających tożsamość osoby oraz ich kserowanie. Dodatkowo, działaniem naruszającym prywatność było sporządzanie kserokopii całego (wówczas książeczkowego) dowodu osobistego, zawierającego także informacje ze sfery prywatności, całkowicie nieprzydatne do ustalenia tożsamości klienta, dotyczące np. miejsc

[6] Por. sprawy prowadzone przez Generalnego Inspektora Ochrony Danych Osobowych GI-DS-430/150/06, GI-DS-430/167/06 (por. *Sprawozdanie z działalności GIODO w roku 2006*, www.giodo.gov.pl, s. 37–38).

[7] Por. sprawy prowadzone przez GIODO z 2006 r.: GI-DS-430/224/06, czy GI-DS-430/250/06 (*Sprawozdanie z działalności…*, *op.cit.*, (www.giodo.gov.pl, s. 37).

[8] Wyrok NSA II SA/Wa 1252/07.

zatrudnienia w przeszłości, miejsc zameldowania, czy dat urodzenia dzieci[9]. Po zmianie przepisów prawa telekomunikacyjnego, wyraźnie wyliczającego zakres przetwarzanych danych klientów, okazało się, że przedstawiciele operatorów sieci telefonicznych nie muszą już potwierdzać tożsamości i kserować wielu dokumentów zawierających różne dane dotyczące klienta, mimo, iż dane zawarte w nowym dowodzie osobistym są stosunkowo ograniczone. Natomiast problem adekwatności (odpowiedniości) danych do celu przetwarzania ciągle pojawia się w działalności banków, które żądając wielu informacji, nie tylko potwierdzających zdolność kredytową klienta, ale i stosunki rodzinne, czy dotyczących wydarzeń z przeszłości, wkraczają nadmiernie w prywatność klientów. Z punktu widzenia przepisów o ochronie danych osobowych jest to działanie naruszające art. 26 ustawy nakazujący administratorowi ochronę interesów osób, których dane są przetwarzane, natomiast z punktu widzenia klientów jest to nieuzasadnione i naruszające prywatność, a zatem nieetyczne postępowanie przedsiębiorcy.

Inną formą naruszenia praw klientów, wynikających z ustawy o ochronie danych osobowych, jest przetwarzanie danych bez dopełnienia obowiązku informacyjnego w jakimkolwiek zakresie. W przypadkach będących przedmiotem skarg do GIODO, podmioty gospodarcze rejestrujące działalność za granicą (najczęściej w USA), prowadziły promocję produktów i usług w tzw. „systemie wysyłkowym" nie informując klientów o swoim statusie i adresie, celu przetwarzania, czy źródle danych. Uniemożliwiało to skarżącym nie tylko złożenie żądania usunięcia danych i np. nie przekazywania ich innym podmiotom, ale ustalenie, skąd dane zostały uzyskane. Działania takich podmiotów połączone bywały z ofertą „nagród pieniężnych", pod warunkiem dokonania zakupu określonego produktu bądź towarów „po promocyjnej cenie", które to oferty bądź w ogóle nie były realizowane mimo dokonywania zakupów bądź przesyłania pieniędzy lub – jak się okazywało – były niekorzystne dla kupujących[10]. Pisma od firm sformułowane bywały także jako „decyzje o przyznaniu dotacji", „decyzje wypłaty", czy informacji, że została przyznana wysoka wygrana. Jednakże, żeby ją odebrać odbiorca musiał spełnić kilka warunków, np. zadzwonić pod podany numer telefonu (koszt połączenia za minutę wahał się od kilku do kilkunastu złotych)[11]. Działania takie i im podobne należy zakwalifikować jako zwykłe oszustwo na szkodę klientów.

Do rażących naruszeń praw klientów należy również brak weryfikacji i aktualizacji danych będących w dyspozycji administratora. Przetwarzanie danych merytorycznie poprawnych i adekwatnych do celów, wynikających z ustawy o ochronie danych, należy nie tylko do obowiązków administratora danych, ale jest ważnym instrumentem ochrony interesów klientów. Tymczasem, ze skarg kierowanych do organu ochrony danych osobowych wynika, że nawet podmioty, które powinny dokładać szczególnej staranności w ochronie interesów klientów (banki i inne instytucje bankowe), przetwarzały nieaktualne dane o klientach banków (kredytobiorcach), co narażało klientów na konkretne straty w postaci np. odmów udzielania kredytów jako osobom zadłużonym. Przyczyną takich działań były nie tylko problemy techniczne z funkcjonowaniem systemu informatycznego, np. brak spójno-

[9] Por. sprawy GI-DIS – 130/99/539, GI-DIS-245/99/654 czy GI-DP-445/99/451 (*Sprawozdanie z działalności Generalnego Inspektora Ochrony Danych Osobowych za okres 01.01.1999 r. – 31.12.1999 r.* – wyd. GIODO, s. 118).

[10] Sprawa GI-DS-430/465/04.

[11] Por sprawy GI-DS-430/91/04, GI-DS-430/130/04 (*Sprawozdanie Generalnego Inspektora Ochrony Danych Osobowych z działalności za rok 200*4, s. 199).

ści systemów informatycznych banków z systemem Biura Informacji Kredytowej, ale także zwykłe zaniechanie ze strony banków, które prowadziło do tego, że aktualizacja danych następowała po wielu miesiącach. Przykładem może być sprawa, w której aktualizacja danych – w postaci przekazania do rejestru Biura Informacji Kredytowej informacji o spłaceniu kredytu – nastąpiła dopiero po 18 miesiącach i dotyczyła 55 tysięcy klientów[12].

Inny charakter – strat moralnych – miały sprawy dotyczące wykorzystywania nie zaktualizowanych zbiorów danych przez firmy marketingowe. Gdyby firmy, zgodnie z ustawą o ochronie danych osobowych, w przypadku zbierania danych nie od osoby, której dotyczą, najpierw dopełniały obowiązku informacyjnego po uzyskaniu danych, a później dopiero podejmowały działania marketingowe, to mogłyby zweryfikować i zaktualizować dane, usuwając nie tylko informacje o osobach, które nie wyrażają zgody na wykorzystywanie ich danych, ale usuwając dane osób zmarłych. Niewykonywanie obowiązków ustawowych sprawiało, iż zdarzało się, że oferty marketingowe kierowane były do osób zmarłych, co było szczególnie przykrym przeżyciem dla najbliższych członków rodziny, zwłaszcza wówczas, gdy osoba najbliższa nie żyła już od pewnego czasu, a oferta marketingowa sformułowana w dość bezpośredniej formie[13] sugerowała, jakoby zmarły w ciągu ostatnich tygodni aktywnie uczestniczył w „grze", właśnie „przeszedł do trzeciego etapu" i czeka na niego nagroda.

Odrębnym problemem jest wykonywanie obowiązku właściwego zabezpieczenia danych. Nie zabezpieczenie danych stanowi nie tylko naruszenie przepisów ustawy o ochronie danych osobowych, ale może prowadzić do ich udostępnienia osobom nieuprawnionym, mogącym wykorzystać dane ze szkodą dla osób, których dane dotyczą. Owo niewykonanie obowiązku zabezpieczenia danych może przyjmować formę braku odpowiednich urządzeń technicznych (np. braku stosowanego zabezpieczenia systemu informatycznego), niezastosowanie wskazanych w ustawie i przepisach wykonawczych procedur i dokumentów związanych z zabezpieczeniem danych, ale może także wynikać z braku wiedzy pracowników podmiotu gospodarczego o konieczności ochrony danych, bądź lekceważenia przez nich obowiązków pracowniczych. Zdarzające się w praktyce przypadki znajdowania informacji o klientach, np. w formie wydruków z bankowych systemów informatycznych na śmietniku lub w miejscach publicznych, wskazują na lekceważenie problemu bezpieczeństwa danych, a tym samym – na lekceważenie klientów, o których informacje zostały upublicznione w taki sposób[14]. Szczególnie drastycznym przykładem lekceważenia klientów jest porzucanie dokumentacji dotyczącej klientów w przypadku likwidacji firmy, czy oddziału firmy. Może to świadczyć również o braku profesjonalizmu pracowników podmiotu gospodarczego, zwłaszcza wówczas, gdy udostępnione dane nie dotyczą jedynie informacji identyfikujących osobę, ale dotyczą jej stanu zdrowia (przypadki wyrzucania bez anonimizacji dokumentów medycznych), czy stanu posiadania (wydruki bankowe). Brakiem profesjonalizmu pracowników, ale także – jak można przypuszczać – wynikiem niedopełnienia obowiązku szkolenia pracowników przez pracodawców, czy stosowania

[12] *Sprawozdanie GIODO za rok 2006*, (www.giodo.gov.pl) s. 32.

[13] W ofertach używano imion osób, np. „*Panie Władysławie przeszedł Pan do trzeciego etapu i wygrał 50 tys. złotych*".

[14] Takie przypadki szczególnie często zdarzały się w początkowym okresie obowiązywania ustawy o ochronie danych osobowych. Przykładem mogą być sprawy opisane w sprawozdaniu GIODO za rok 1999. Por. *Sprawozdanie z działalności generalnego Inspektora Ochrony Danych Osobowych za okres 01.01.1999 – 31.12.1999*, wyd. GIODO, s.136–137; Do tej pory media donoszą o porzuceniu dokumentów zawierających dane osobowe, np. klientów banku.

odpowiednich procedur, można tłumaczyć przypadki wykorzystywania służbowych systemów informatycznych do prowadzenia prywatnej korespondencji przy wykorzystaniu służbowego internetu. Efektem takiego działania może być ułatwienie tzw. hakerom dostępu do firmowego systemu informatycznego, a w efekcie dostęp do wielu danych o klientach, kradzieże danych, czy kradzieże pieniędzy z kont bankowych klientów.

Naruszenia praw klientów są rażące szczególnie wówczas, gdy prowadzenie działalności gospodarczej oparte jest z założenia na wzajemnym zaufaniu przedsiębiorcy i klientów. Nie zabezpieczenie bankowego systemu informatycznego, bądź prowadzenie działalności marketingowej przez bank na rzecz innych podmiotów gospodarczych, jest odbierane przez klientów jako działanie szczególnie nieetyczne – z uwagi na powszechne traktowanie banków jako podmiotów zaufania publicznego.

Wyrazem działania naruszającego normy etyczne jest również udostępnianie przedstawicielom mediów informacji o klientach, w tym informacji objętych inną jeszcze tajemnicą, np. tajemnicą telekomunikacyjną. Jako przykład można powołać udostępnienie przez operatora sieci telefonicznej informacji o połączeniach i treści rozmów pomiędzy osobą w sprawie której toczyło się postępowanie przed sejmową komisja śledczą, a innymi osobami z którymi przeprowadzała ona rozmowy, która to treść rozmów została później opublikowana w dzienniku „Rzeczpospolita".

5. Praktyka stosowania ustawy o ochronie danych osobowych dostarczyła wiele przykładów – z których jedynie niektóre przytoczone zostały w niniejszym tekście – świadczących nie tylko o niewykonywaniu obowiązków wynikających z ustawy o ochronie danych osobowych, ale o braku etyki w kontaktach z klientami. I jakkolwiek przy omawianiu przykładów naruszeń praw klientów, w wielu przypadkach używana była forma czasu przeszłego, to stwierdzić należy, że nieetyczne i naruszające prawa osób praktyki podmiotów gospodarczych w dalszym ciągu nie należą do rzadkości[15].

Uniemożliwianie skorzystania z przysługujących praw, w tym z prawa kontroli przetwarzania danych, niepodawanie adresu siedziby firmy, żeby uniemożliwić dotarcie do firmy osobom, których dane zostały wykorzystane bądź organom kontrolującym, nie zabezpieczenie danych i nie stosowanie wymaganych przepisami prawa procedur, nie zabezpieczenie dokumentów zawierających dane osobowe, czy po prostu ich porzucanie, brak aktualizowania danych klientów banków w rejestrach Biura Informacji Kredytowej, posługiwanie się nie zweryfikowanymi zbiorami danych i przesyłanie ofert marketingowych do osób zmarłych, to kilka z licznych przykładów działań na szkodę klientów, podważających zaufanie do podmiotów gospodarczych i naruszających dobra osobiste, a nawet narażających klientów na szkody materialne. Z kolei, wprowadzanie w błąd klientów co do celu przetwarzania danych, przekazywanie danych innym podmiotom, sprzedaż zbiorów danych, czy zgoła handlowanie danymi gromadzonymi w innym celu, jest nie tylko działaniem nieetycznym, ale dostarcza przedsiębiorcom nieuzasadnionych zysków kosztem praw klientów.

Trudno jest jednoznacznie określić przyczyny takiego zachowania przedsiębiorców. Niewątpliwie przyczyn należy szukać w lekceważeniu obowiązującego prawa, zarówno

[15] Przykładem mogą być choćby opisywane niedawno przez prasę działania kancelarii zajmujących się uzyskiwaniem odszkodowań na rzecz ofiar wypadków drogowych, które kupują nielegalnie nazwiska ofiar wypadków bądź wykorzystują stan szoku powypadkowego ofiar do wyłudzania podpisów na umowach upoważniających do prowadzenia spraw o uzyskanie odszkodowania za odpowiednio wysoką prowizję (Por. np. artykuł *Ucywilizować łowców nieszczęść*, [w:] „Gazeta Wyborcza" z dnia 23 lipca 2009 r., s. 2.

przez podmioty łamiące prawo, jak i organy ścigania, które na znaczną większość zawiadomień o podejrzeniu popełnienia przestępstwa odpowiadały informacją o niepodjęciu postępowania bądź o umorzeniu postępowania ze względu na znikomość społecznej szkodliwości czynu sprawcy. Reakcja prokuratury jest o tyle uderzająca, że chodzi o naruszenia przepisów chroniących konstytucyjnie zagwarantowane prawo obywateli.

Można mieć jednak nadzieję, że w miarę upływu czasu sytuacja w Polsce zmieni się na tyle, że opisywane w niniejszym tekście przypadki nie będą miały miejsca.

Personal Data Protection as an Ethical Aspect of Entrepreneurship

Summary

The Personal Data Protection Act was enacted in 1997; it imposed some obligations on all the administrators of personal data regardless if acting as private or public establishments. The Act was intended to guarantee the safety of personal data and to ensure the right to controlling the data processing.

However, since the enacting of the Act, there have been reported instances of its infringement, especially by private entrepreneurs.

The numerous appealed complaints show that the entrepreneurs neglect their duty of ensuring the safety of personal data (e.g. documents or media with such personal data), which results in unauthorised revealing the data to third parties. An especially serious case of the infringements of the Act and the rights of the persons concerned is selling the data without a person's consent. In many cases the administrator only seemingly informs about the purposes of processing the data and then, in this or any other insidious way (among them an inacceptable presumption of consent), beguiles the necessary acceptance.

The occurrences of neglecting duties imposed by the Act are to be considered not only as infringement of law, but also as unethical actions resulting in undermining customers' confidence in entrepreneurs. For example: The unprotected data can be viewed and used by unauthorised parties to the detriment of the persons concerned (e. g. identity theft). The selling of the data is also a source of an unjustifiable profit for an entrepreneur and makes controlling of the processing of personal data impossible. Even if there are no negative consequences for the customer, the cases of infringement the Personal Data Protection Act bring about to undermine confidence not only in the entrepreneur (the source of personal data) but also in private establishments in general.

Translated by *Tomasz Nowacki*