Aldona Wnęk, Katarzyna Policha

Ochrona danych osobowych i innych danych prawnie chronionych w sektorze ubezpieczeń. Zagadnienia wybrane

1. Wstęp

W dniu 7 marca 2011 r. weszła w życie ustawa z dnia 29 października 2010 r. o zmianie ustawy o ochronie danych osobowych oraz niektórych innych ustaw[1] (u.o.d.o.). Nowelizacja ta – jak wynika z uzasadnienia[2] – stanowi kolejny krok w procesie implementacji dyrektywy Parlamentu Europejskiego i Rady 95/46/WE z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych[3].

Najważniejsze zmiany, wprowadzone tą nowelizacją**,** dotyczą dwóch obszarów normatywnych. Pierwszy obszar obejmuje kwestie merytoryczne – zasady postępowania przy przetwarzaniu danych osobowych oraz kwestie praw osób fizycznych, których dane osobowe są lub mogą być przetwarzane w zbiorach danych. Drugi obszar zmian dotyczy wyposażenia Generalnego Inspektora Ochrony Danych Osobowych (GIODO) w nowe – skuteczniejsze od dotychczas stosowanych – instrumenty egzekwowania prawa, co powinno służyć zwiększeniu rzeczywistej ochrony danych osobowych w Polsce.

W pierwszym obszarze przede wszystkim należy zwrócić uwagę na zmianę dokonaną w art. 7 pkt 5 u.o.d.o. Doprecyzowana została mianowicie definicja zgody na przetwarzanie danych – wskazano, że **zgoda ta może być w każdym czasie odwołana.** W dotychczasowym stanie prawnym zagadnienie możliwości odwołania zgody nie było interpretowane w sposób jednolity. Z jednej strony argumentowano, że zgoda na przetwarzanie danych – jako oświadczenie woli – może być w każdej chwili odwołana na podstawie przepisów ogólnych. Argumentacja ta nie była jednak przyjmowana powszechnie, ponieważ w praktyce występowały sytuacje, w których osobom zainteresowanym odma-

[1] Dz. U. Nr 229, poz. 1497.
[2] www.sejm.gov.pl
[3] Dz. Urz. WE L 281 z 23.11.1995, s. 31 z późn. zm.; Dz. Urz. UE Polskie wydanie specjalne, rozdz. 13, t. 15, s. 355 z późn. zm.

wiano możliwości skorzystania z możliwości (uprawnienia) odwołania zgody. Po dokonanej zmianie przepisów uprawnienie do odwołania zgody nie budzi wątpliwości – przepis ustawy jest jednoznaczny, zatem osoba zainteresowana może powołać się na konkretny przepis.

Kolejna istotna zmiana dotyczy **uchylenia art. 29**. Przepis ten regulował udostępnianie danych osobowych w celach innych niż włączenie do zbioru. Dotyczył m.in. udostępnienia danych na wniosek osoby, która w sposób wiarygodny uzasadniła potrzebę posiadania tych danych, przy założeniu, że ich udostępnienie nie naruszało praw i wolności osób, których dane dotyczyły. Uchylenie art. 29 wynika z faktu, iż uznano (zgodnie zresztą ze stanowiskiem Komisji Europejskiej), że zwolnienie z zasady ograniczonego celu jest dopuszczalne jedynie dla utrzymania porządku publicznego. Dlatego też wiarygodne uzasadnienie potrzeby posiadania danych osobowych nie powinno stanowić samoistnej przesłanki udostępnienia danych osobie trzeciej[4].

Drugi obszar to nowe regulacje, których skutkiem jest **zwiększenie zakresu kompetencji Generalnego Inspektora Ochrony Danych Osobowych.** W wyniku zmiany art. 12 pkt 3 u.o.d.o. zadania GIODO uzupełniono o obowiązek zapewnienia wykonania obowiązków o charakterze niepieniężnym, wynikających z wydawanych przez GIODO decyzji administracyjnych, przez stosowanie środków egzekucyjnych przewidzianych w ustawie z dnia 17 czerwca 1966 r. o postępowaniu egzekucyjnym w administracji[5]. GIODO uzyskał zatem status organu egzekucyjnego w zakresie egzekucji administracyjnej obowiązków o charakterze niepieniężnym. Oznacza to, że będzie on uprawniony do stosowania środków egzekucyjnych, przede wszystkim grzywny, w celu przymuszenia (art. 121 tej ustawy). Grzywna może być nakładana kilkakrotnie w tej samej lub w wyższej kwocie: wysokość grzywny może wynosić maksymalnie 10 000 zł w stosunku do osoby fizycznej i 50 000 zł w stosunku do osoby prawnej oraz jednostki organizacyjnej nieposiadającej osobowości prawnej; w przypadku wielokrotnego nakładania grzywny w jednym postępowaniu egzekucyjnym ich łączna kwota nie może przekroczyć 50 000 zł w odniesieniu do osoby fizycznej i 200 000 zł w odniesieniu do osoby prawnej oraz jednostki organizacyjnej nieposiadającej osobowości prawnej.

W nowym art. 19a zawarto regulację, zgodnie z którą – w celu realizacji zadań polegających na inicjowaniu i podejmowaniu przedsięwzięć w zakresie doskonalenia ochrony danych osobowych – GIODO może kierować do organów

[4] Nowelizacja wprowadziła także zmiany o charakterze porządkowym. W art. 33 ust. 1 skreślono katalog danych, do przekazania których był zobowiązany administrator danych wobec osoby, której dane dotyczą (było to powtórzenie innych przepisów u.o.d.o.). W art. 34 wskazano przesłanki odmowy udzielenia przez administratora danych informacji osobie realizującej prawo kontroli przetwarzania danych. W art. 41 ust. 1 pkt 2 skonkretyzowano podmiot obowiązany do zgłoszenia zbioru danych do rejestracji (administrator danych) oraz doprecyzowano i usystematyzowano wymagane informacje objęte zgłoszeniem zbioru danych do rejestracji. W tym samym artykule ponadto dodano ust. 3 i 4 w celu podkreślenia, że w przypadku danych szczególnie chronionych (dane wrażliwe) administrator danych ma obowiązek zgłosić zmianę w zbiorze przed jej dokonaniem.

[5] Dz. U. z 2005 r. Nr 229, poz. 1954 z późn. zm.

państwowych, organów samorządu terytorialnego, państwowych i komunalnych jednostek organizacyjnych, podmiotów niepublicznych realizujących zadania publiczne, osób fizycznych i prawnych, jednostek organizacyjnych niebędących osobami prawnymi oraz innych podmiotów – wystąpienia zmierzające do zapewnienia skutecznej ochrony danych osobowych. GIODO może również występować do właściwych organów z wnioskami o podjęcie inicjatywy ustawodawczej albo o wydanie bądź zmianę aktów prawnych w sprawach dotyczących ochrony danych osobowych. Podmiot, do którego zostało skierowane takie wystąpienie lub wniosek, jest obowiązany ustosunkować się do nich na piśmie w terminie 30 dni od daty otrzymania.

Wobec obserwowanego w praktyce GIODO niedostatecznego wykorzystywania dopuszczalnych środków karnych, w art. 54a stypizowane zostało nowe przestępstwo, polegające na udaremnianiu lub utrudnianiu GIODO wykonywania czynności kontrolnych, co koreluje ze zmianami w zakresie kontroli wprowadzonymi w art. 15 i 16 u.o.d.o. (zakres upoważnienia do przeprowadzenia kontroli, wymagania dotyczące protokołu kontroli).

2. Gromadzenie i przetwarzanie danych osobowych

Omawiana nowelizacja ustawy o ochronie danych osobowych jest właściwą okazją do ponownej, praktycznej analizy zagadnień związanych z gromadzeniem i przetwarzaniem danych prawnie chronionych w sektorze ubezpieczeń, w tym danych osobowych.

Przechodząc na grunt u.o.d.o. należy przede wszystkich wskazać, że legalność przetwarzania danych osobowych (tzw. zwykłych) uzależniona jest od spełnienia przez administratora danych jednej z **przesłanek** wskazanych w art. 23 ust. 1 u.o.d.o., zaś w przypadku tzw. danych wrażliwych – w art. 27 ust. 2 u.o.d.o. W przypadku zakładów ubezpieczeń zasadniczymi przesłankami będą te wskazane w art. 23 ust. 1 u.o.d.o.: pkt 1 (zgoda osoby, której dane dotyczą), pkt 2 (przetwarzanie danych jest niezbędne do zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa) oraz pkt 3 (przetwarzanie danych jest konieczne do realizacji umowy, gdy osoba, której dane dotyczą, jest jej stroną lub gdy jest to niezbędne do podjęcia działań przed zawarciem umowy na żądanie osoby, której dane dotyczą). Granice realizacji tych przesłanek wyznacza ustawa z dnia 22 maja 2003 r. o działalności ubezpieczeniowej[6] (u.d.u.) oraz wydane na jej podstawie akty wykonawcze. Ponadto zgodnie z zasadą adekwatności, o której mowa w art. 26 ust. 1 pkt 3 u.o.d.o., zakres danych przetwarzanych przez administratora musi być adekwatny, tzn. proporcjonalny do celu ich przetwarzania, natomiast przetwarzanie danych w zakresie szerszym niż niezbędny do zawarcia, a następnie realizacji umowy, może odbywać się wyłącznie za zgodą osoby, której dane dotyczą (art. 23 ust. 1 pkt 1 u.o.d.o.).

W sposób szczególny uregulowano przetwarzanie przez zakłady ubezpieczeń informacji o stanie zdrowia. Zgodnie z art. 22 ust. 1 u.d.u.

[6] Tekst jedn. Dz. U. z 2010 r. Nr 11, poz. 66 z późn. zm.

zakład ubezpieczeń może uzyskać odpłatnie od podmiotów, wymienionych w art. 4 tej ustawy, które udzielały świadczeń zdrowotnych ubezpieczonemu lub osobie, na rzecz której miała być zawarta umowa ubezpieczenia, informacje o okolicznościach związanych z oceną ryzyka ubezpieczeniowego i weryfikacją podanych przez tę osobę danych o jej stanie zdrowia, ustaleniem prawa tej osoby do świadczenia z zawartej umowy ubezpieczenia i wysokością tego świadczenia, a także informacje o przyczynie śmierci ubezpieczonego, z wyłączeniem wyników badań genetycznych. Na podstawie ust. 3 wystąpienie zakładu ubezpieczeń z wnioskiem o udzielenie ww. informacji wymaga pisemnej zgody ubezpieczonego lub osoby, na rzecz której ma zostać zawarta umowa ubezpieczenia, albo jej przedstawiciela ustawowego.

Przetwarzanie przez zakłady ubezpieczeń danych osobowych klientów w **celach marketingowych** własnych usług i produktów ubezpieczeniowych dopuszczalne jest na podstawie przesłanki, o której mowa w art. 23 ust. 1 pkt 5 u.o.d.o. Zgodnie z tym przepisem przetwarzanie takie jest dopuszczalne, gdy jest ono niezbędne do wypełnienia prawnie usprawiedliwionych celów realizowanych przez administratorów danych albo odbiorców danych, a przetwarzanie nie narusza praw i wolności osoby, której dane dotyczą, przy czym stosownie do ust. 4 pkt 1 za prawnie usprawiedliwiony cel uważa się w szczególności marketing bezpośredni własnych produktów lub usług administratora danych. Wobec tego należy podkreślić, że w tym przypadku zgoda klienta nie jest wymagana. Będzie ona natomiast wymagana, jeżeli zakład ubezpieczeń zamierza przetwarzać dane osobowe klientów w celu promocji produktów lub usług podmiotu trzeciego. Ważne jest zapewnienie, aby zgoda była wyraźna i dotyczyła przetwarzania danych w konkretnym celu, określonym przez administratora danych, ze wskazaniem podmiotu lub grupy podmiotów, których marketing miałby dotyczyć. Zgoda powinna być wyraźnie oddzielona od celu realizacji umowy.

Agent ubezpieczeniowy działający w imieniu i na rzecz zakładu ubezpieczeń[7] nie jest administratorem zbioru danych osobowych osób, wobec których występuje jako przedstawiciel zakładu ubezpieczeń. Agent nie musi w związku z tym legitymować się samodzielną (tzn. odrębną od posiadanej przez zakład ubezpieczeń) przesłanką legalności przetwarzania danych. Agent – jako podmiot, któremu zakład ubezpieczeń w drodze zawartej umowy powierzył przetwarzanie danych[8] – uprawniony jest do przetwarzania tych danych wyłącznie w zakresie i w celu określonym w tej umowie. Zobowiązany jest także do zabezpieczenia danych zgodnie z wymogami u.o.d.o. Natomiast w przypadku przetwarzania przez agenta ubezpieczeniowego danych osobowych potencjalnych klientów spoczywać będą na nim (jako administratorze danych) wszystkie obowiązki wynikające z u.o.d.o.; dotyczy to przede wszystkim obowiązku wykazania przez agenta, na jakiej podstawie dane przetwarza.

---

[7] Art. 7 i nast. ustawy z dnia 22 maja 2003 r. o pośrednictwie ubezpieczeniowym (Dz. U. Nr 124, poz. 1154 z późn. zm.).

[8] Art. 31 u.o.d.o.

W przypadku **brokera ubezpieczeniowego**[9]**, działającego w imieniu i na rzecz podmiotu poszukującego ochrony ubezpieczeniowej, należy odróżnić dwie sytuacje. Broker przetwarza dane na podstawie przesłanki określonej w art. 23 ust.1 pkt 1 u.o.d.o. (zgoda osoby, której dane dotyczą) w przypadku potencjalnych klientów albo na podstawie art. 23 ust. 1 pkt 3 (przetwarzanie danych jest konieczne do realizacji umowy, gdy osoba, której dane dotyczą, jest jej stroną lub gdy jest to niezbędne do podjęcia działań przed zawarciem umowy na żądanie osoby, której dane dotyczą).**

W sytuacji przetwarzania przez brokerów danych osobowych klientów w celach marketingowych ma zastosowanie analogiczna zasada, jak w przypadku zakładów ubezpieczeń, tj. przetwarzanie własnych produktów i usług odbywa się na mocy art. 23 ust. 1 pkt 5 u.o.d.o., a natomiast marketing produktów i usług podmiotów trzecich – wyłącznie za zgodą osoby, której dane mają być przetwarzane.

Jak wspomniano, **w wyniku nowelizacji u.o.d.o. wprowadzono wyraźny przepis uprawniający do odwołania zgody**. Jednakże uprawnieniu temu nie nadano charakteru bezwzględnego. Po pierwsze, nie można cofnąć zgody, jeśli podmiot przetwarzający dane dysponuje już danymi niezbędnymi do wykonania ważnej umowy. Umowa taka – a wraz z nią przetwarzanie danych – zakończyć się może w drodze wypowiedzenia, czy upływu okresu, na jaki została zawarta. Sytuacja tożsama zaistnieje w przypadku danych niezbędnych do dokonania rozliczenia z osobą, która wyraziła zgodę na ich przetwarzanie. Natomiast w przypadku zgody udzielonej w celach niezwiązanych bezpośrednio z wykonaniem umowy (np. cele marketingowe, przekazywanie danych innym podmiotom) możliwe jest odwołanie zgody, chociaż sama umowa pozostaje w mocy.

W tym kontekście pojawia się istotne zagadnienie związane z faktem, iż w praktyce zakłady ubezpieczeń pobierają oświadczenia o zgodzie na przetwarzanie danych osobowych nawet w przypadkach, gdy istnieją inne przesłanki przetwarzania tych danych. W związku z tym należy rozważyć, jakie konsekwencje będzie miało odwołanie zgody złożonej w takich okolicznościach, to znaczy, czy w przypadku odwołania zgody dane osobowe mogą być dalej przetwarzane na podstawie innych przesłanek. Sprowadza się to do rozstrzygnięcia kwestii, czy można przyjąć, że skoro zgoda została uznana za przesłankę przetwarzania, wyłącza ona stosowanie pozostałych przesłanek, w związku z czym odwołanie zgody uniemożliwia ich dalsze przetwarzanie? Wydaje się, że taka interpretacja byłaby za daleko idąca. Należy pamiętać, że przesłanki przetwarzania danych mają charakter równorzędny i każda z nich stanowi samodzielną podstawę przetwarzania danych. Jednak nie eliminuje to kolejnego problemu o niezwykłej doniosłości praktycznej, mianowicie jeśli klient odwołał zgodę, wyraził przez to w sposób wyraźny swoją wolę zaprzestania przetwarzania jego danych, ale z drugiej strony –

[9] Art. 20 i nast. ustawy z dnia 22 maja 2003 r. o pośrednictwie ubezpieczeniowym.

wobec istnienia innych przesłanek przetwarzania – odwołanie zgody nie wywoła skutków prawnych.

3. Szczególna ochrona danych

Przetwarzanie danych osobowych, także w sektorze ubezpieczeń, odbywa się zatem co do zasady na podstawie przepisów u.o.d.o. Wątpliwości powstają jednak w sferze relacji tej ustawy z innymi przepisami, które w sposób odrębny regulują ochronę danych – na tle art. 5 u.o.d.o. Zgodnie z tym przepisem, jeżeli uregulowania odrębnych ustaw, które odnoszą się do przetwarzania danych, przewidują dalej idącą ochronę niż wynika z u.o.d.o., to stosuje się przepisy tych ustaw. W doktrynie wskazuje się, że jest to szczególny przypadek **normy kolizyjnej** *lex specialis derogat legi generali* (norma szczególna pozbawia mocy normę ogólną), przy czym ma pierwszeństwo przed innymi regułami kolizyjnymi. Wobec tego przepisy przewidujące ochronę dalej idącą wyłączają stosowanie u.o.d.o. tylko w zakresie, w jakim ta ochrona jest szersza. Implikuje to konieczność każdorazowego badania, czy odmienne uregulowanie zapewnia dalej idącą ochronę niż wynikająca z u.o.d.o. Natomiast stwierdzenie, że przepis szczególny przewiduje ochronę słabszą niż wynikająca z u.o.d.o., powoduje automatyczne stosowanie reżimu u.o.d.o.

Powyższe zagadnienie nabiera szczególnej ostrości przy analizie **dopuszczalności przetwarzania przez zakłady ubezpieczeń danych szczególnie chronionych** (w tym danych dotyczących zdrowia). Należy pamiętać, że u.o.d.o. szeroko definiuje przetwarzanie danych jako wykonywanie jakichkolwiek operacji na danych (zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie), przy czym przetwarzanie danych osobowych zawsze wymaga uzasadnienia, stąd ustawowe przesłanki ich przetwarzania. W przypadku danych wrażliwych (dane dotyczące pochodzenia rasowego lub etnicznego, poglądów politycznych, przekonań religijnych lub filozoficznych, przynależności wyznaniowej, partyjnej lub związkowej, stanu zdrowia, kodu genetycznego, nałogów, życia seksualnego, skazań, orzeczeń o ukaraniu, mandatów karnych oraz innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym) u.o.d.o. wprowadza generalny zakaz ich przetwarzania, z wyjątkiem przypadków ściśle określonych w tej ustawie. Przetwarzanie danych wrażliwych jest możliwe, gdy osoba, której dane dotyczą, **wyrazi zgodę na piśmie na ich przetwarzanie.** Jest ono także dopuszczalne, gdy przepis szczególny innej ustawy zezwala na przetwarzanie danych wrażliwych bez zgody osoby, której one dotyczą, z zastrzeżeniem, iż przepis ten stwarza pełne gwarancje ich ochrony. W świetle powyższego należy stwierdzić, że u.o.d.o. stwarza surowsze wymogi dla zgody na przetwarzanie danych wrażliwych niż kodeks cywilny dla oświadczenia woli. Zgodnie z art. 60 k.c.[10], z zastrzeżeniem wyjątków przewidzianych w ustawie, wola osoby dokonującej czynności prawnej może być wyrażona przez każde zachowanie się tej osoby, które ujawnia jej wolę w sposób dostateczny, w tym również przez ujawnienie tej woli

[10] Ustawa z dnia 23 kwietnia 1964 r. – Kodeks cywilny (Dz. U. Nr 16, poz. 93 z późn. zm.).

w postaci elektronicznej (oświadczenie woli). Ustawa o ochronie danych osobowych zastrzega wymóg formy pisemnej takiego oświadczenia. Zgoda ta nie może być domniemana lub dorozumiana z oświadczenia woli o innej treści. Z treści oświadczenia powinno w sposób niebudzący wątpliwości wynikać, w jakim celu, w jakim zakresie i przez kogo dane osobowe (dane wrażliwe) będą przetwarzane.

Jak wspomniano, na podstawie ustawy o działalności ubezpieczeniowej zakład ubezpieczeń może przetwarzać dane wrażliwe. Artykuł 24 u.d.u. stanowi podstawę do zbierania danych (przy czym przepis ten nie wskazuje ich rodzaju ani zakresu) w celu oceny ryzyka ubezpieczeniowego lub wykonania umowy ubezpieczenia, zawartych w umowach ubezpieczenia lub oświadczeniach ubezpieczających składanych przed zawarciem umowy, danych ubezpieczonych lub uprawnionych z umowy ubezpieczenia. Powstaje pytanie**, czy art. 24 u.d.u. stanowi podstawę do przetwarzania – bez konieczności uzyskiwania pisemnej zgody klientów – również danych wrażliwych, które są jednymi z podstawowych danych wykorzystywanych w underwritingu medycznym.** Dopuszczenie takiej możliwości powoduje doniosłe skutki praktyczne, w szczególności ułatwienie dystrybucji produktów ubezpieczeniowych za pomocą środków porozumiewania się na odległość. W związku z art. 5 u.o.d.o. należy stwierdzić, że ustawa ta stwarza dalej idącą ochronę danych wrażliwych niż art. 24 u.d.u. Jak wskazuje GIODO, **odstąpienie od generalnego zakazu przetwarzania danych osobowych wrażliwych jest możliwe jedynie w sytuacji, gdy inna ustawa wyraźnie zezwala na przetwarzanie danych wrażliwych**, tzn. m.in. na ich udostępnienie określonym podmiotom bądź na ich zbieranie i wykorzystywanie przez wskazane podmioty; takim przykładem są np. przepisy o kontroli skarbowej[11], o Policji[12] czy o Służbie Celnej[13].

Powyższy przykład nie wyczerpuje katalogu problemów praktycznych, które pojawiają się w bieżącej działalności zakładów ubezpieczeń. Część z nich była przedmiotem wyjaśnień GIODO[14].

4. Zasady zbierania danych osobowych. Obowiązek informacyjny

Realizując zasadę celowości przetwarzania danych przepisy u.o.d.o. normują procedurę zbierania danych osobowych (jako jednej z form przetwarzania danych), w tym pobieranie danych bez wiedzy osób, których dane dotyczą, oraz szczególne **obowiązki informacyjne** jako warunki legalności zbierania danych. Istotą obowiązku informacyjnego jest udzielenie osobie, której gromadzone dane osobowe dotyczą, minimalnego (określonego przez ustawodawcę)

[11] Art. 7c ust. 1 ustawy z dnia 28 września 1991 r. o kontroli skarbowej (Dz. U. z 2011r. Nr 41, poz. 214 z późn. zm.).
[12] Art. 14 ust. 4 oraz art. 20 ust. 2a–2c ustawy dnia 6 kwietnia 1990 r. o Policji (Dz. U. z 2007 r. Nr 43, poz. 277 z późn. zm.).
[13] Art. 7 ust. 1 oraz art. 75c ustawy z dnia 27 sierpnia 2009 r. o Służbie Celnej (Dz. U. Nr 168, poz. 1323 z późn. zm.).
[14] www.giodo.gov.pl

zakresu informacji, na podstawie których osoba ta może podjąć świadomą decyzję co do ujawnienia i udostępnienia danych.

Zgodnie z art. 24 u.o.d.o. w przypadku zbierania danych osobowych **od osoby**, której one dotyczą, administrator danych jest obowiązany poinformować tę osobę o adresie swojej siedziby i pełnej nazwie, a w przypadku gdy administratorem danych jest osoba fizyczna – o miejscu swojego zamieszkania oraz imieniu i nazwisku, celu zbierania danych, a w szczególności o znanych mu w czasie udzielania informacji lub przewidywanych odbiorcach lub kategoriach odbiorców danych, prawie dostępu do treści swoich danych oraz ich poprawiania, a także dobrowolności albo obowiązku podania danych, a jeżeli taki obowiązek istnieje – o jego podstawie prawnej. Wyjątek stanowią przypadki, gdy przepis innej ustawy zezwala na przetwarzanie danych bez ujawniania faktycznego celu ich zbierania lub osoba, której dane dotyczą, posiada informacje w ww. zakresie. Ponadto, art. 32 ust. 4 u.o.d.o. stanowi, iż administrator danych może odstąpić od informowania osób o przetwarzaniu ich danych w przypadkach, gdy dane są przetwarzane do celów naukowych, dydaktycznych, historycznych, statystycznych lub archiwalnych, a dopełnienie obowiązku informacyjnego pociągałoby za sobą nakłady niewspółmierne z zamierzonym celem. Ww. przepis dotyczy tzw. bezpośredniego zbierania danych, niezależnie od środka (technicznego), jakim się w danym przypadku posłużono (telefon, poczta elektroniczna, ankieta). Administrator danych powinien udzielić określonych informacji przed udostępnieniem mu danych osobowych. Wniosek taki wynika z art. 23 u.o.d.o., określającego przesłanki przetwarzania danych. Ważne jest stwierdzenie, że obowiązek obejmuje wyłącznie podanie informacji identyfikujących administratora danych, natomiast nie dotyczy podmiotu, który zbiera dane na jego rzecz.

Artykuł 25 u.o.d.o. dotyczy zbierania danych osobowych **nie od osoby, której one dotyczą** (pośrednie zbieranie danych). W rozumieniu tego przepisu źródłem danych może być zarówno osoba trzecia (tzn. osoba inna niż osoba, której dane dotyczą), jak i dokumenty (w tym wykazy, spisy, rejestry). Obowiązek informacyjny aktualizuje się w każdej sytuacji, w której administrator pozyskuje dane niebędące dotąd w jego posiadaniu (także w przypadku rozszerzenia zbioru danych). Administrator danych jest wobec tego obowiązany poinformować osobę, której dane dotyczą, bezpośrednio po utrwaleniu zebranych danych, o adresie swojej siedziby i pełnej nazwie, a w przypadku, gdy administratorem danych jest osoba fizyczna – o miejscu swojego zamieszkania oraz imieniu i nazwisku, celu i zakresie zbierania danych, a w szczególności o odbiorcach lub kategoriach odbiorców danych, źródle danych, prawie dostępu do treści swoich danych oraz ich poprawiania, a także o uprawnieniach dotyczących żądania zaprzestania przetwarzania danych lub sprzeciwu wobec ich przetwarzania w przypadkach wskazanych w u.o.d.o. (chodzi o art. 23 ust. 1 pkt 4 i 5, gdy przetwarzanie danych jest niezbędne do wykonania określonych prawem zadań realizowanych dla dobra publicznego lub, gdy jest niezbędne dla wypełnienia prawnie usprawiedliwionych celów realizowanych przez administratorów danych albo odbiorców danych, a przetwarzanie nie narusza praw

i wolności osoby, której dane dotyczą). **Wyjątki dotyczą przede wszystkim sytuacji, gdy przepis innej ustawy przewiduje lub dopuszcza zbieranie danych osobowych bez wiedzy osoby, której dane dotyczą – takim przepisem jest art. 24 u.d.u.**, zgodnie z którym zakład ubezpieczeń jest zwolniony z obowiązku informacyjnego w stosunku do określonej kategorii osób (ubezpieczonych lub uprawnionych z umowy ubezpieczenia) w zakresie zbierania ich danych zawartych w umowach ubezpieczenia lub oświadczeniach ubezpieczających składanych przed zawarciem umowy.

Kolejne wyjątki dotyczą sytuacji, gdy dane są niezbędne do badań naukowych, dydaktycznych, historycznych, statystycznych lub badania opinii publicznej, ich przetwarzanie nie narusza praw lub wolności osoby, której dane dotyczą, a spełnienie ww. wymagań wymagałoby nadmiernych nakładów lub zagrażałoby realizacji celu badania, dane są przetwarzane przez administratora wskazanego w u.o.d.o. na podstawie przepisów prawa lub osoba, której dane dotyczą, posiada ww. informacje.

Istotne jest zastrzeżenie, że powstanie obowiązku informacyjnego administratora następuje po utrwaleniu danych. Dlatego też nie można uznać za dozwolone jednoczesnego wysłania informacji mającej na celu wykonanie obowiązku z art. 25 u.o.d.o. wraz z ofertą marketingową – oznaczałoby to sytuację, w której dany podmiot przetwarzałby dane osobowe (do celów złożenia oferty marketingowej) przed dopełnieniem obowiązku informacyjnego wynikającego z art. 25 u.o.d.o. **W świetle ww. przepisów należałoby uznać, iż obowiązki informacyjne powstają po stronie każdego podmiotu, który z danych korzysta.**

Pośrednie zbieranie danych odgrywa ważną rolę w sektorze ubezpieczeń; dzieje się tak przede wszystkim z uwagi na działające na naszym rynku grupy kapitałowe, a także nabiera ono istotnego znaczenia w przypadku **zakładów reasekuracji.** Brak przepisów w tym zakresie powoduje, że powstają istotne wątpliwości zarówno natury prawnej, jak i praktycznej. Jak się wydaje, podstawę przetwarzania danych przez zakłady reasekuracji stanowi art. 19 ust. 2 pkt 21a u.d.u. (szerzej na temat tajemnicy ubezpieczeniowej w dalszej części artykułu). Przepis ten dopuszcza (na warunkach w nim określonych) przekazanie zakładowi reasekuracji, tj. ujawnienie mu przez zakład ubezpieczeń, danych dotyczących umowy ubezpieczenia; wśród nich znajdują się także dane osobowe. Ujawnienie to skutkuje po stronie zakładu reasekuracji możliwością przetwarzania danych w zakresie umów ubezpieczenia ryzyka objętych **konkretną umową reasekuracji** (przy czym zakres dozwolonego przetwarzania nie został wskazany). Przyjęcie powyższej tezy ma doniosłe znaczenie z punktu widzenia realizacji przez zakłady reasekuracji obowiązku informacyjnego, o którym mowa w art. 25 ust. 1 u.o.d.o. Jeżeli art. 19 ust. 2 pkt 21a u.d.u. uznamy w sposób niebudzący wątpliwości za podstawę przetwarzania danych przez zakłady reasekuracji – będą one zwolnione z tego obowiązku na podstawie art. 25 ust. 2 pkt 1 u.o.d.o., zgodnie z którym w przypadku zbierania danych osobowych nie od osoby, której one dotyczą, administrator danych jest zwolniony z obowiązku informacyjnego wobec tej osoby

(który musi być dopełniony bezpośrednio po utrwaleniu zebranych danych), jeżeli przepis innej ustawy przewiduje lub dopuszcza zbieranie danych osobowych bez wiedzy osoby, której dane dotyczą (szerzej na ten temat w dalszej części artykułu).

Wydaje się jednak, że powyższa kwestia wymaga jednoznacznego rozstrzygnięcia ustawodawcy, z uwzględnieniem specyfiki działalności reasekuracyjnej; **przepis taki powinien znaleźć się w ustawie o działalności ubezpieczeniowej. Jest to pożądane tym bardziej, że brak regulacji szczególnych może wskazywać na brak takiego wyłączenia.** Omawiane wyłączenie zostało wprowadzone w u.d.u. wobec zakładów ubezpieczeń (zgodnie z art. 24 ust. 2 u.d.u. zbieranie danych, o których mowa w tym przepisie, odpowiednio w celu oceny ryzyka ubezpieczeniowego lub wykonania umowy ubezpieczenia przez zakład ubezpieczeń, nie powoduje po stronie zakładu ubezpieczeń obowiązku powiadomienia, o którym mowa w art. 25 ust. 1 u.o.d.o.).

Dalszym problemem jest kwestia, czy art. 19 ust. 2 pkt 21a u.d.u. dotyczy **retrocesji** – co prawda w tym przypadku mamy także do czynienia z zakładem reasekuracji i umową reasekuracji, ale zawieraną pomiędzy innymi podmiotami niż te, o których mowa w u.d.u. – art. 19 ust. 2 pkt 21a odnosi się do umowy reasekuracji zwolnienia zakładu ubezpieczeń z tajemnicy ubezpieczeniowej wobec zakładu reasekuracji, ale w zakresie umów reasekuracji pomiędzy tym zakładem ubezpieczeń i zakładem reasekuracji.

5. Tajemnica ubezpieczeniowa – zagadnienia praktyczne

Przepisy o ochronie danych osobowych nie wyczerpują problematyki dostępu do danych prawnie chronionych w sektorze ubezpieczeń.

Artykuł 19 u.d.u. reguluje **tajemnicę ubezpieczeniową**, określając przede wszystkim w sposób enumeratywny podmioty obowiązane do jej zachowania, tj. zakład ubezpieczeń, osoby w nim zatrudnione oraz osoby i podmioty, za pomocą których zakład ubezpieczeń wykonuje czynności ubezpieczeniowe. Ta ostatnia grupa obejmuje podmioty, którym zlecono wykonywanie określonych czynności ubezpieczeniowych w zakresie, w jakim podmioty te wykonują określone czynności *„w imieniu i na rzecz zakładu ubezpieczeń”* – w przeciwnym razie czynności te w ogóle nie stanowią czynności ubezpieczeniowych; należą do niej m.in. **agenci ubezpieczeniowi**, którzy – zgodnie z art. 13 ust. 1 pkt 3 ustawy o pośrednictwie ubezpieczeniowym – są zobowiązani zachować w tajemnicy nie tylko informacje dotyczące indywidualnych umów ubezpieczenia, ale wszelkie informacje uzyskane w związku z wykonywaniem czynności agencyjnych, dotyczące zarówno zakładu ubezpieczeń, jak i drugiej strony umowy ubezpieczenia oraz podmiotu szukającego ochrony ubezpieczeniowej.

W świetle u.d.u. tajemnica ubezpieczeniowa obejmuje poszczególne umowy ubezpieczenia, a więc zakres danych szerszy niż tylko dane osobowe. Przyjmuje się, że tajemnicą ubezpieczeniową objęty jest cały stosunek prawny ubezpieczenia, w tym również sam fakt zawarcia umowy ubezpieczenia, dane dotyczące osób objętych tym stosunkiem w jakimkolwiek

charakterze (ubezpieczający, ubezpieczony, uposażony lub uprawniony do otrzymania świadczenia ubezpieczeniowego) oraz wszelkie informacje, jakie zakład ubezpieczeń otrzymał w związku z oferowaniem i zawarciem danej umowy ubezpieczenia. Uznaje się, że tajemnicą ubezpieczeniową objęte są również informacje, które zakład ubezpieczeń otrzymuje w związku z podejmowaniem czynności zmierzających do zawarcia umowy, które jednak nie doprowadziły do jej zawarcia. Tajemnica ubezpieczeniowa nie dotyczy danych zbiorczych o charakterze statystycznym, które nie zawierają informacji pozwalających na zidentyfikowanie poszczególnych umów ubezpieczenia.

Możliwość przekazywania danych objętych tajemnicą ubezpieczeniową została ograniczona do podmiotów wskazanych w u.d.u. (jak wspomniano katalog ww. podmiotów ma charakter zamknięty) i obejmuje z jednej strony instytucje publiczne w zakresie ich kompetencji wynikających z odrębnych przepisów, z drugiej – podmioty, wobec których uchyla się tajemnicę w celu umożliwienia wykonywania określonych czynności (ubezpieczeniowych).

Kolejny doniosły problem praktyczny dotyczy tego, czy podmiot upoważniony do otrzymania danych na podstawie art. 19 ust. 2 u.d.u. może je udostępnić dalszemu podmiotowi **(tzw. upoważnienie kaskadowe).** Kwestia ta jest obecnie sporna. Z jednej strony przepis u.d.u. ustanawia zamknięty podmiotowo katalog uprawnionych. Z drugiej jednak strony – jak się wydaje – przepis ten należy odczytywać w kontekście potencjalnych stosunków istniejących między podmiotem uprawnionym a podmiotem, któremu ten udostępnia dane. Jeżeli dalszy podmiot nie działa w imieniu własnym, lecz w imieniu i na rachunek podmiotu uprawnionego, należałoby takie „dalsze" przekazanie danych uznać za dopuszczalne. Zwraca też uwagę, iż podmiotowy charakter upoważnienia z art. 19 ust. 2 u.d.u. powoduje, że upoważnione są podmioty jako organizacje – instytucje, wobec czego w ramach takiego podmiotu upoważniona jest każda osoba, której działania można danemu podmiotowi przypisać.

Z tajemnicą ubezpieczeniową pozostaje w ścisłym związku także zagadnienie **dostępu zakładów ubezpieczeń do danych zgromadzonych przez inne podmioty**. Wiąże się to w szczególności z postulowanym (przede wszystkim przez Rzecznika Ubezpieczonych) uregulowaniem zasad takiego dostępu na poziomie ustawowym (tak, jak miało to miejsce w przypadku danych o stanie zdrowia, zgodnie z art. 21–23 u.d.u.), co w sposób znaczący powinno przyczynić się do uproszczenia i usprawnienia działalności zakładów ubezpieczeń i zwiększenia efektywności oraz poprawy standardu obsługi klienta zarówno na etapie zawierania umowy (oceny ryzyka), jak i wypłaty odszkodowania lub świadczenia. W obecnym stanie prawnym, zgodnie z art. 24–25 u.d.u., zakład ubezpieczeń może zbierać – odpowiednio w celu oceny ryzyka ubezpieczeniowego lub wykonania umowy ubezpieczenia – zawarte w umowach ubezpieczenia lub oświadczeniach ubezpieczających składanych przed zawarciem umowy dane ubezpieczonych lub uprawnionych z umowy ubezpieczenia. Sądy, prokuratura, Policja oraz inne organy i instytucje, na wniosek zakładu ubezpieczeń, w zakresie zadań przez ten zakład ubezpieczeń wykonywanych i w celu ich wykona-

nia, w związku z wypadkiem lub zdarzeniem będącym podstawą ustalania odpowiedzialności, udzielają informacji o stanie sprawy oraz udostępniają zebrane materiały, jeżeli są one niezbędne do ustalenia okoliczności tych wypadków i zdarzeń losowych oraz wysokości odszkodowania lub świadczenia. Ponadto sądy, prokuratura, Policja oraz inne organy i instytucje, na wniosek Ubezpieczeniowego Funduszu Gwarancyjnego, Polskiego Biura Ubezpieczycieli Komunikacyjnych lub Rzecznika Ubezpieczonych, w ramach zadań przez nie wykonywanych i w celu ich wykonania, udzielają informacji w zakresie stanu sprawy oraz udostępniają zebrane materiały[15].

6. Kierunki regulacji danych osobowych

Jak wynika z dotychczasowych rozważań, wielość reżimów prawnych, którym podlega przetwarzanie danych przez zakłady ubezpieczeń, powoduje znaczne trudności w praktyce. **W wielu obszarach pożądane jest wprowadzenie jasnego i spójnego uregulowania przetwarzania danych w sektorze ubezpieczeń, co zwiększyłoby pewność prawa i ułatwiło jego stosowanie, a w sposób oczywisty byłoby korzystne zarówno z perspektywy zapewnienia odpowiedniego poziomu ochrony przetwarzania danych osobowych klientów, jak i zakładów ubezpieczeń.** Powyższy **postulat** dotyczy w szczególności następujących zagadnień.

Jak wspomniano, zgodnie z art. 27 ust. 2 pkt 1 u.o.d.o. przetwarzanie danych wrażliwych jest dopuszczalne m.in. w przypadku wyrażenia zgody na piśmie przez osobę, której dane dotyczą. Tymczasem art. 8 ust. 2 przytoczonej wyżej dyrektywy 95/46/WE[16] wymaga, aby zgoda na przetwarzanie danych wrażliwych była udzielona „wyraźnie". Nie przewiduje przy tym żadnej szczególnej formy. Zastrzeżenie formy pisemnej powoduje w praktyce daleko idące konsekwencje, np. przy zawieraniu umów ubezpieczenia przez telefon czy drogą elektroniczną.

Artykuł 31 u.o.d.o. dotyczy powierzenia przetwarzania danych osobowych. Podmioty przyjmujące dane korzystają z usług wyspecjalizowanych dalszych podmiotów, np. z zakresu informatyki, niszczenia danych itp. W praktyce uznano, że taka możliwość istnieje w świetle obowiązujących przepisów, jeżeli wyraźnie wynika z umowy powierzenia przetwarzania danych. Wydaje się konieczne rozważenie wprowadzenia przepisu, który wprost dawałby taką możliwość.

---

[15] Dotychczasowy stan prawny ogranicza w tym zakresie możliwości zakładów ubezpieczeń. Jako przykład można wskazać przepisy ustawy z dnia 29 września 1986 r. – Prawo o aktach stanu cywilnego (Dz. U. z 2004 r. Nr 161, poz. 1688 z późn. zm.). Zgodnie z art. 83 ust. 2 tej ustawy odpisy aktów stanu cywilnego i zaświadczenia o dokonanych w księgach stanu cywilnego wpisach lub o ich braku mogą być wydane na wniosek osób, które wykażą w tym interes prawny. W praktyce zakłady ubezpieczeń spotykają się z odmową udostępnienia tego typu dokumentów, ponieważ nie są uznawane za podmioty, które mogą wykazać interes prawny; dotyczy to w szczególności odmowy udostępnienia karty zgonu, która zawiera stwierdzenie przyczyny zgonu (stanowi podstawę sporządzenia aktu zgonu). Powyższy przykład nie ma charakteru jednostkowego, dotyczy wielu sfer podlegających odrębnej ochronie (np. tajemnica zawodowa).

[16] Patrz przypis 3.

W związku z postępującym procesem globalizacji coraz większego znaczenia nabiera zagadnienie transgranicznego przekazywania danych. Przekazywanie danych do krajów należących do Europejskiego Obszaru Gospodarczego podlega temu samemu reżimowi, co przetwarzanie danych na terytorium Polski (państwa członkowskie EOG zapewniają adekwatny poziom ochrony danych, zgodnie z postanowieniami dyrektywy 95/46/WE). Według art. 47–48 u.o.d.o. przekazanie danych osobowych do innego państwa, tzw. państwa trzeciego, może nastąpić, jeżeli państwo docelowe daje gwarancje ochrony danych osobowych na swoim terytorium przynajmniej takie, jakie obowiązują na terytorium Rzeczypospolitej Polskiej. Przepisu tego nie stosuje się, gdy przesłanie danych osobowych wynika z obowiązku nałożonego na administratora danych przepisami prawa lub postanowieniami ratyfikowanej umowy międzynarodowej. Administrator danych może jednak przekazać dane osobowe do państwa trzeciego, jeżeli osoba, której dane dotyczą, udzieliła na to zgody na piśmie; przekazanie jest niezbędne do wykonania umowy pomiędzy administratorem danych a osobą, której dane dotyczą, lub jest podejmowane na jej życzenie; przekazanie jest niezbędne do wykonania umowy zawartej w interesie osoby, której dane dotyczą, pomiędzy administratorem danych a innym podmiotem; przekazanie jest niezbędne ze względu na dobro publiczne lub do wykazania zasadności roszczeń prawnych; przekazanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą; dane są ogólnie dostępne. W pozostałych przypadkach przekazanie danych osobowych do państwa trzeciego, które nie daje gwarancji ochrony danych osobowych przynajmniej takich, jakie obowiązują na terytorium Rzeczypospolitej Polskiej, może nastąpić po uzyskaniu zgody GIODO, pod warunkiem że administrator danych zapewni odpowiednie zabezpieczenia w zakresie ochrony prywatności oraz praw i wolności osoby, której dane dotyczą. **Naruszenie przez zakład ubezpieczeń tych zasad jest równoznaczne z naruszeniem przepisów o tajemnicy ubezpieczeniowej**.

W tym kontekście powstaje także **problem transferu danych niebędących danymi osobowymi poza granice Polski.** Kwestia ta – w przeciwieństwie do transferu danych osobowych – nie została uregulowana w przepisach. Z drugiej strony – jak wspomniano – tajemnicą ubezpieczeniową objęte są wszelkie dane dotyczące poszczególnych umów ubezpieczenia (nie tylko dane osobowe). Nie powinno budzić wątpliwości, że zawarte w u.d.u. zasady dotyczące udostępniania danych objętych tajemnicą ubezpieczeniową mają zastosowanie również do danych niebędących danymi osobowymi, a dotyczących umów ubezpieczenia. Wątpliwość powstaje jednak wobec możliwości przetwarzania danych niebędących danymi osobowymi w zakresie nieuregulowanym w u.d.u. **Brak jest wyraźnych podstaw prawnych do przetwarzania, w tym przesyłania do krajów trzecich, danych niebędących danymi osobowymi, znajdujących się w posiadaniu zakładów ubezpieczeń.**

7. Ochrona danych w zakresie usług świadczonych drogą elektroniczną

Dla zakładów ubezpieczeń – zwłaszcza prowadzących działalność w systemie *direct* z wykorzystaniem systemów teleinformatycznych – szczególne znaczenie ma ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną[17] (u.ś.u.d.e.), zwłaszcza art. 16–22 tej ustawy, dotyczące zasady ochrony danych osobowych. Na podstawie ww. ustawy podlegają ochronie dane usługobiorców usługi świadczonej drogą elektroniczną, będących osobami fizycznymi (np. ubezpieczający zawierający umowę ubezpieczenia w systemie *direct*). Usługodawcą w rozumieniu u.ś.u.d.e. jest podmiot, który – prowadząc choćby ubocznie działalność zarobkową lub zawodową – świadczy usługi drogą elektroniczną, przy czym chodzi zarówno o podmiot, który udostępnia usługi własne, jak i pośredniczy w dostępie do tych usług. Jednak tylko podmiot udostępniający usługi własne decyduje o celu i środkach przetwarzania danych, wobec tego konieczne jest uzyskanie przez ten podmiot statusu administratora danych w rozumieniu art. 7 u.o.d.o.

W kontekście art. 5 u.o.d.o., **ustawa o świadczeniu usług drogą elektroniczną jest aktem prawnym zapewniającym dalej idącą ochronę przetwarzania danych osobowych niż wynikająca z u.o.d.o.** Do przetwarzania danych osobowych w rozumieniu ustawy o ochronie danych osobowych w związku ze świadczeniem usług drogą elektroniczną stosuje się przepisy ustawy o świadczeniu usług drogą elektroniczną, o ile ustawa ta nie stanowi inaczej. Istotna odrębność ochrony danych w tym reżimie wynika z tego, iż dane osobowe podlegają ochronie przewidzianej w u.ś.u.d.e. w zakresie ich przetwarzania niezależnie od tego, czy jest ono dokonywane w zbiorach danych (w przeciwieństwie do u.o.d.o.). Dane osobowe usługobiorcy mogą być przetwarzane przez usługodawcę w celu i zakresie określonym w u.ś.u.d.e., przy czym chodzi o dane w niej wymienione, a niezbędne do nawiązania, ukształtowania treści, zmiany lub rozwiązania stosunku prawnego między nimi: nazwisko i imiona usługobiorcy, numer ewidencyjny PESEL lub – gdy ten numer nie został nadany – numer paszportu, dowodu osobistego lub innego dokumentu potwierdzającego tożsamość, adres zameldowania na pobyt stały, adres do korespondencji, jeżeli jest inny niż adres, o którym mowa w pkt 3, dane służące do weryfikacji podpisu elektronicznego usługobiorcy, adresy elektroniczne usługobiorcy. W celu realizacji umów lub dokonania innej czynności prawnej z usługobiorcą, usługodawca może przetwarzać inne dane niezbędne ze względu na właściwość świadczonej usługi lub sposób jej rozliczenia.

Usługodawca jest zobowiązany do wyróżnienia i oznaczenia określonych w u.ś.u.d.e. danych jako takich, których podanie jest niezbędne do świadczenia usługi drogą elektroniczną, przy czym na tle tych rozwiązań powstają wątpliwości wynikające z odmienności, co do wskazanych – odmiennych – przesłanek

[17] Dz. U. Nr 144, poz. 1204 z późn. zm.

uzasadniających niezbędność przetwarzania danych, implikujących odmienność w zakresie samej kategorii danych, których przetwarzanie jest niezbędne.

Usługodawca może przetwarzać, za zgodą usługobiorcy i do celów określonych powyżej także inne dane dotyczące usługobiorcy, które nie są niezbędne do świadczenia usługi drogą elektroniczną. Sporne jest, czy uzyskanie zgody podmiotu, którego dane podlegają przetwarzaniu, jest wystarczające dla przetwarzania wszelkich kategorii danych.

Odrębną kategorią danych są tzw. **dane eksploatacyjne**, tj. charakteryzujące sposób korzystania przez usługobiorcę z usługi świadczonej drogą elektroniczną z tym, że usługodawca może przetwarzać następujące dane eksploatacyjne: oznaczenia identyfikujące usługobiorcę nadawane na podstawie ww. danych, oznaczenia identyfikujące zakończenie sieci telekomunikacyjnej lub system teleinformatyczny, z którego korzystał usługobiorca, informacje o rozpoczęciu, zakończeniu oraz zakresie każdorazowego korzystania z usługi świadczonej drogą elektroniczną, informacje o skorzystaniu przez usługobiorcę z usług świadczonych drogą elektroniczną. Usługodawca udziela informacji o danych organom państwa na potrzeby prowadzonych przez nie postępowań. **Nie może on przetwarzać danych osobowych usługobiorcy po zakończeniu korzystania z usługi świadczonej drogą elektroniczną**, poza wyjątkami wskazanymi w ustawie (chodzi m.in. o dane niezbędne do rozliczenia usługi oraz dochodzenia roszczeń z tytułu płatności za korzystanie z usługi). Rozliczenie usługi świadczonej drogą elektroniczną przedstawione usługobiorcy nie może ujawniać rodzaju, czasu trwania, częstotliwości i innych parametrów technicznych poszczególnych usług, z których skorzystał usługobiorca, chyba że zażądał on szczegółowych informacji w tym zakresie. Dla celów reklamy, badania rynku oraz zachowań i preferencji usługobiorców (z przeznaczeniem wyników tych badań na potrzeby polepszenia jakości usług świadczonych przez usługodawcę), za zgodą usługobiorcy, **dopuszcza się jedynie zestawianie danych** przetwarzanych za zgodą usługobiorcy. Dotyczy to jednak tylko wybranych danych, a ponadto warunkiem ich zestawiania jest usunięcie wszelkich oznaczeń identyfikujących usługobiorcę albo system teleinformatyczny, z którego usługodawca korzystał (**anonimizacja danych**). Usługodawca nie może zestawiać danych osobowych usługobiorcy z przybranym przez niego pseudonimem. **Usługodawca, który przetwarza dane osobowe usługobiorcy, jest obowiązany zapewnić mu dostęp do aktualnej informacji** o możliwości korzystania z usługi świadczonej drogą elektroniczną anonimowo lub z wykorzystaniem pseudonimu, udostępnianych przez usługodawcę środkach technicznych zapobiegających pozyskiwaniu i modyfikowaniu przez osoby nieuprawnione danych osobowych przesyłanych drogą elektroniczną, podmiocie, któremu powierza przetwarzanie danych, ich zakresie i zamierzonym terminie przekazania, jeżeli usługodawca zawarł z tym podmiotem umowę o powierzenie do przetwarzania określonych danych. Informacje te powinny być dla usługobiorcy stale i łatwo dostępne za pomocą systemu teleinformatycznego, którym się posługuje.

W przypadku uzyskania przez usługodawcę wiadomości o korzystaniu przez usługobiorcę z usługi świadczonej drogą elektroniczną niezgodnie z regulaminem lub z obowiązującymi przepisami (niedozwolone korzystanie), usługodawcy przysługują wobec usługobiorcy określone uprawnienia. Przede wszystkim może on przetwarzać dane osobowe usługobiorcy w zakresie niezbędnym do ustalenia odpowiedzialności usługobiorcy, pod warunkiem że utrwali – dla celów dowodowych – fakt uzyskania oraz treść tych wiadomości.

8. Ochrona danych a przeciwdziałanie praniu pieniędzy

Gromadzenie danych osobowych wynika także z przepisów **o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu**[18].

Zakłady ubezpieczeń prowadzące działalność w zakresie ubezpieczeń na życie mają status tzw. instytucji obowiązanych. W związku z tym są zobowiązane do stosowania wobec swoich klientów środków bezpieczeństwa finansowego, polegających m.in. na identyfikacji i weryfikacji tożsamości klienta. W sytuacjach podwyższonego ryzyka prania pieniędzy lub finansowania terroryzmu wymagane jest stosowanie wzmożonych środków bezpieczeństwa finansowego; dotyczy to sytuacji, gdy klient jest nieobecny przy zawieraniu umowy (np. zawieranie umów ubezpieczenia na życie w systemie *direct*). W świetle art. 9e ww. ustawy, w przypadku zawierania umów ubezpieczenia na życie z wykorzystaniem środków teleinformatycznego porozumiewania się na odległość, zakład ubezpieczeń zobowiązany jest podjąć, obok podstawowych środków bezpieczeństwa finansowego, również co najmniej jeden z następujących dodatkowych środków: ustalenie tożsamości klienta na podstawie dodatkowych dokumentów lub informacji, dodatkową weryfikację autentyczności przedstawionych dokumentów lub poświadczenie ich zgodności z oryginałem przez notariusza, organ administracji rządowej, organ samorządu terytorialnego lub podmiot świadczący usługi finansowe, ustalenie, że pierwsza transakcja została przeprowadzona za pośrednictwem rachunku klienta w podmiocie świadczącym usługi finansowe.

Niedopełnienie tych obowiązków przez zakłady ubezpieczeń wiąże się z ryzykiem naruszenia przepisów ustawy, co w konsekwencji może doprowadzić do nałożenia kar pieniężnych przez Generalnego Inspektora Informacji Finansowej.

9. Podsumowanie

Z powyższych rozważań wynika w sposób jednoznaczny, że wielość reżimów prawnych w zakresie danych prawnie chronionych, w których funkcjonują podmioty sektora ubezpieczeń, powoduje istotne trudności interpretacyjne, co przekłada się na stosowanie ww. przepisów w praktyce, zwłaszcza w obszarach, w których dochodzi do styku różnych reżimów ochrony. Podane przykłady prak-

[18] Ustawa z dnia 16 listopada 2000 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (Dz. U. z 2010 r. Nr 46, poz. 276 z późn. zm.).

tyczne nie wyczerpują katalogu potencjalnych zagadnień, które mogą wystąpić w ich bieżącej działalności.

Należy niewątpliwie postulować wprowadzenie kompleksowych uregulowań dotyczących zasad przetwarzania danych, w tym danych wrażliwych, z uwzględnieniem także zakresu obowiązku informacyjnego realizowanego wobec zainteresowanych przez zakłady ubezpieczeń i inne podmioty rynku ubezpieczeń. Dotychczasowe regulacje mają w większości charakter doraźny i cząstkowy. Odrębną kwestię stanowi funkcjonowanie baz danych budowanych przez Polską Izbę Ubezpieczeń czy Ubezpieczeniowy Fundusz Gwarancyjny.

Z uwagi na wzajemne powiązania w sektorze finansowym należy także postulować spójność między przepisami funkcjonującymi w poszczególnym sferach tego sektora. Jako przykład można wskazać wspomniane przepisy dotyczące tajemnicy bankowej, które w sposób zdecydowanie pełniejszy regulują zasady dostępu do danych objętych tą tajemnicą. ■

Protection of Personal Data and Other Legally Protected Data in Insurers' Activity. Selected Issues

This article is a comprehensive as well as practical presentation concerning the collection and processing of legally protected personal data in the insurance sector, in which large databases are kept.

Firstly, the authors discuss the changes introduced by the latest amendment to the Data Protection Act of 29 October 2010 related to the rules of conduct for the personal data processing, as well as increasing the scope of the tasks of the General Inspector for the Personal Data Protection. The impact has been presented of the above-mentioned modifications upon the existing provisions regulating the basis and principles of the processing of personal data by the insurance sector operators (insurance companies, agents and brokers), with particular emphasis on the processing of sensitive data, including health status data, which are essential for medical underwriting. Furthermore, the authors show several practical problems concerning the application of the regulations on the protection of personal data in the context of other provisions regulating legally protected data (Insurance Activity Act). Moreover, a separate part of the article is devoted to the responsibilities of information data administrators. Also, de lege ferenda postulates related to the desired statutory changes have some practical value. Then, the issue of insurance secrecy is discussed as well as the data protection in electronic services.

The final part of the article is devoted to the anti-money laundering and combating the financing of terrorism regulations in the context of the operation of life insurance companies and their role as so-called "obligated institutions".