

Karol Rajewski

Funkcja *compliance* w strukturze organizacyjnej zakładów ubezpieczeń – wyzwania i aspekty praktyczne

Zarządzanie zgodnością działalności przedsiębiorstwa z szeroko pojętymi przepisami prawa oraz innymi normami, określane mianem *compliance*, odgrywa coraz większą rolę w zakładach ubezpieczeń. Podstawowym celem tej funkcji – jako jednej z kluczowych funkcji systemu zarządzania ryzykiem oraz elementu systemu kontroli wewnętrznej – jest wypracowanie takiej organizacji zakładu ubezpieczeń i współpracy wszystkich pracowników, aby uzyskać pewność, że procesy biznesowe odbywają się zgodnie z regulacjami prawnymi, rekomendacjami i wytycznymi regulatorów, strategią oraz deklarowanymi wartościami etycznymi.

Autor przedstawia wybrane zagadnienia kluczowe dla zarządzania ryzykiem *compliance* w zakładzie ubezpieczeń. Omawia relacje pomiędzy funkcją *compliance* a innymi komórkami organizacyjnymi oraz organem nadzoru. Ramy opracowania pozwalają jedynie na przedstawienie struktury zagadnień, które stoją przed *compliance* w zmieniającej się sytuacji rynkowej. Niektóre z przedstawionych aspektów powinny być oczywiście rozwinięte, ale to wymaga, w ocenie autora, odrębnych opracowań.

Słowa kluczowe: *compliance*, system zarządzania zakładem ubezpieczeń, funkcje kluczowe, kontrola wewnętrzna, zarządzanie ryzykiem *compliance*.

1. Polityka zarządzania zgodnością (*compliance*) w zakładach ubezpieczeń

Przed zarządzającymi polityką zarządzania zgodnością – *compliance* w zakładach ubezpieczeń pojawiają się coraz większe wyzwania w kontekście nałożonych przez nowe regulacje obowiązków związanych z tą funkcją oraz nowych obowiązków przypisanych do kontroli wewnętrznej. Nie mniej istotnym źródłem nowych zadań stojących przed *compliance* są coraz ambitniejsze cele biznesowe, strategie, wartości, z którymi muszą zmierzyć się zakłady ubezpieczeń¹. Na nowe otoczenie biznesowe ma wpływ nie tylko rozwój nowych technologii², ale i nowe regulacje prawne oraz konsekwencje głośnych postępowań sądowych, wpływających na reputację całego rynku, jak np. skargi klientów i postępowania Urzędu Ochrony Konkurencji i Konsumentów prowadzone w sprawie tzw. polisolatek i ubezpieczeń z funduszami inwestycyjnymi. Przy czym chodzi tu nie tylko o samo zbudowanie lub uzupełnienie tzw. systemów *compliance*, ale przede wszystkim zapewnienie, że procesy bizneso-

¹ Wybrane pozycje z bogatej literatury na temat *compliance* przedstawiono w bibliografii. Warto śledzić tę problematykę w kwartalniku „Compliance i Zarządzanie” (Magazyn Fachowy Instytutu Compliance) – darmowym czasopiśmie online.

² K. Rajewski, „Wyzwania i bariery w procesie digitalizacji”. Compliance – Magazyn Fachowy Instytutu Compliance, czerwiec 2017, nr 2, s. 28–31.

we odbywają się zgodnie z założonymi celami, strategią oraz deklarowanymi wartościami. Kluczowe dla osiągnięcia takiego stanu jest zagwarantowanie i wyegzekwowanie, aby wszyscy pracownicy i przedstawiciele zakładów ubezpieczeń znali, rozumieli i stosowali przepisy prawa, zasady polityk wewnętrznych i przyjęte zasady biznesowe. **Takie prowadzenie biznesu jest wymierną w dłuższej perspektywie wartością dla akcjonariuszy firm ubezpieczeniowych, wpływa pozytywnie na rynek usług ubezpieczeniowo-finansowych oraz jest jednym z istotniejszych czynników wzrostu dla tego sektora.** Za jeden z przykładów takiego pozytywnego wpływu może posłużyć usprawnienie przez podmioty rynku finansowo-ubezpieczeniowego procesu obsługi skarg, informowania klientów w odpowiedni sposób o sprzedawanych produktach i ich powiązaniu z potrzebami klientów oraz efektywna obsługa klientów już po zakupie przez nich produktów ubezpieczeniowych. Przykładem badania takiego wzrostu zaufania klientów jest tzw. wskaźnik NPS³.

Za cel wprowadzenia polityki zarządzania zgodnością uznaje się opisanie i przedstawienie zasad oraz struktury organizacyjnej w odniesieniu do funkcji *compliance* jako elementu systemu kontroli wewnętrznej oraz jednej z kluczowych funkcji systemu zarządzania ryzykiem w zakładzie ubezpieczeń. Rekomendowane jest, aby w zakładzie ubezpieczeń został przygotowany i wdrożony dokument opisujący system kontroli wewnętrznej oraz pozostałe kluczowe funkcje. Dokument taki może zostać nazwany „Opisem systemu zarządzania w zakładzie ubezpieczeń”. Zgodnie bowiem z art. 3 ust. 1 pkt 46 ustawy z dnia 11 września 2015 r. o działalności ubezpieczeniowej i reasekuracyjnej⁴ w skład systemu zarządzania zakładem ubezpieczeń wchodzi następujące funkcje: funkcja zarządzania ryzykiem, funkcja zgodności z przepisami, funkcja audytu wewnętrznego i funkcja aktuarialna.

W dalszej części artykułu przedstawione zostaną wybrane zagadnienia kluczowe dla zarządzania ryzykiem *compliance* w zakładzie ubezpieczeń.

2. Ryzyko *compliance* – podział

Warto podkreślić, że niewłaściwe zarządzanie ryzykiem *compliance* prowadzi do pogorszenia reputacji zakładu, a nawet do zastosowania sankcji prawnych mogących skutkować stratami finansowymi. Z tego powodu wyzwaniem dla zarządów firm i służb *compliance* jest takie prowadzenie działalności, które nie spowoduje naruszenia zasad biznesowych oraz przepisów prawnych i innych regulacji odnoszących się do działalności zakładów.

Przyjmuje się cztery główne obszary ryzyka:

- 1) postępowanie klienta,
- 2) postępowanie osobiste,

³ L. Piesik, „Wspomagająca technologia”, *Gazeta Bankowa* 2008, nr 21, s. 57–59, por. uwagi dotyczące ryzyka odnoszącego się do bezpośredniego kontaktu z klientem, zarówno na rynku bankowym, jak i ubezpieczeniowym.

⁴ Dz. U. z 2015 r. poz. 1844, z późn. zm.

- 3) usługi finansowe,
- 4) struktura i działalność organizacji.

2.1. Postępowanie klienta – tożsamość lub zachowanie klientów (FEC/AML)

Zakłady ubezpieczeń jako instytucje finansowe są narażone na wykorzystanie przez przestępców w działaniach o charakterze prania brudnych pieniędzy, a także finansowania terroryzmu, w tym terroryzmu finansowego. Wbrew powszechnemu przekonaniu, że jest to jedynie teoretyczne ryzyko, które realizuje się raczej w działalności banków, należy podkreślić, że w związku z charakterem swojej codziennej działalności zakłady ubezpieczeń są mocno narażone na zaangażowanie się w transakcje powiązane z osobami, instytucjami i krajami objętymi sankcjami, a także kontrolą eksportu. Aby temu zapobiec, stosowane są normy i regulacje na poziomie narodowym, międzynarodowym i europejskim. Dlatego w zakładzie ubezpieczeń powinny być podejmowane odpowiednie działania, aby dostosować się do tych norm i regulacji oraz strzec swojej uczciwości i reputacji. Powinny być zdefiniowane zasady zapobiegania przestępstwom finansowo-gospodarczym oraz zbiory wewnętrznych zasad, w których wyszczególniono podjęte środki oraz działania, które należy przeprowadzić, aby mieć pewność, że zagrożenie zostało zmniejszone do najniższego możliwego poziomu.

Zakład ubezpieczeń zobowiązany jest wyznaczyć osobę na stanowisku *Money Laundering Reporting Officer* (MLRO), która koordynuje wdrożenie i wykonanie polityk z zakresu *Financial Economic Crime* (FEC). W praktyce można się spotkać z różnym podejściem do umiejscowienia MLRO w strukturze organizacyjnej. W tradycyjnym modelu funkcja ta umiejscawiana jest w zespole *compliance*. Najczęstszą trudnością w tym modelu jest zapewnienie odpowiednich zasobów i rozwiązań technicznych do realizacji przewidzianych przez regulacje prawne obowiązków.

Z tego powodu w wielu podmiotach zastosowano inne rozwiązanie – umiejscowiono MLRO w strukturze tzw. operacji, czyli tam, gdzie w praktyce wykonuje się obowiązki przewidziane w regulacjach *Anti-money Laundering* (AML). Nie bez znaczenia jest to, że skoncentrowanie funkcji *compliance* jedynie na kontrolowaniu procesów AML ogranicza jej udział w zarządzaniu ryzykiem *compliance* przy tworzeniu i dystrybuowaniu produktów ubezpieczeniowych. Jest to jeden z najważniejszych dylematów, przed którymi stoi rynek.

Ponieważ walka z przestępczością finansowo-gospodarczą stanowi wspólny obowiązek wszystkich pracowników zakładu ubezpieczeń, wskazane jest prowadzenie odpowiednich szkoleń, które zapewnią, że pracownicy będą świadomi, iż:

- zgodnie z wymogami prawa oraz z zachowaniem należytej staranności szacowane jest ryzyko związane z zawarciem każdej indywidualnej umowy, zgodnie z zasadami „poznaj swojego klienta”;
- procedura weryfikacji każdego partnera, z którym zakład ubezpieczeń zamierza prowadzić interesy, musi być przeprowadzona ze szczególną starannością;

- zakład ubezpieczeń nie nawiąże ani nie będzie podtrzymywać żadnych związków z osobami ani instytucjami mieszczącymi się lub posiadającymi powiązania z organami rządowymi w krajach bardzo wysokiego ryzyka. Te kraje to: Kuba, Iran, Korea Północna, Sudan oraz Syria;
- zakład ubezpieczeń nie akceptuje relacji z osobami powiązanymi z aktami terrorystycznymi. Istniejące relacje zostają zakończone, jeśli jest to (prawnie) możliwe. Zakład ubezpieczeń musi mieć możliwość wykrycia osób o takich powiązaniach (na podstawie publicznie dostępnych wykazów) za pomocą narzędzi „przesiewających” nazwiska;
- pracownicy zakładu ubezpieczeń niezwłocznie zgłaszają wszelkie incydenty związane z przestępczością finansowo-gospodarczą do właściwych osób (z funkcji MLRO).

2.2. Postępowanie osobiste – zachowania pracowników

Zakład ubezpieczeń uchwała następujące polityki wewnętrzne, dotyczące omawianych zagadnień, których wdrożenie powinno w istotny sposób ograniczyć ryzyko, jakie może powstać na gruncie istnienia konfliktów interesów:

- 1) polityki prezentów i rozrywek;
- 2) polityki z zakresu *insider trading* (tzn. polityki dotyczącej osób posiadających informacje cenotwórcze);
- 3) polityki sponsoringu;
- 4) polityki dotyczącej działalności zewnętrznej i interesu zewnętrznego.

Konflikty interesów

Ta sfera zarządzania ryzykiem *compliance* staje się coraz bardziej znacząca, w szczególności ze względu na konieczność zapobiegania nadużyciom finansowym i korupcji. Konflikty interesów mogą m.in. wystąpić, gdy obowiązki zawodowe pracownika ścierają się lub wręcz są w konflikcie z innymi interesami. W zależności od natury tych „innych interesów” rozróżniamy osobisty i organizacyjny konflikt interesów.

W przypadku **osobistego konfliktu interesów może istnieć ryzyko, że osobiste interesy wpłyną niekorzystnie na osąd zawodowy, obowiązki i odpowiedzialność pracownika**. Przykładami osobistych interesów są korzyści finansowe i niepieniężne (np. podarunki, rozrywki) lub też możliwość przyczynienia się pracownika do odniesienia korzyści przez inne osoby. Pracownicy powinni dokładać starań, by unikać sytuacji, które mogłyby prowadzić do konfliktu pomiędzy interesami zawodowymi i osobistymi. Już samo wrażenie zaistnienia konfliktu może mieć szkodliwe skutki. Aby zapewnić pracownikom wytyczne dotyczące postępowania w sytuacjach, z którymi mogą się zetknąć, wdrażane są zasady postępowania w przypadku kilku typów osobistych konfliktów interesów, takich jak prezenty, rozrywka i stanowiska zewnętrzne.

Organizacyjne konflikty interesów zachodzą, gdy pracownik staje wobec dwóch różnych interesów w obrębie organizacji, które są trudne lub wręcz niemożliwe do jednoczesnego pogodzenia. Takie konflikty mogą przybierać różne formy, a wiele z nich stanowi integralną część prowa-

dzenia biznesu. Za przykład może posłużyć sytuacja zaistnienia rozbieżności pomiędzy obsługą klienta a osiągnięciem celu operacyjnego, polegającego na realizacji tej obsługi w ściśle określonym czasie.

Podarunki, rozrywki i posiłki biznesowe, sponsoring i darowizny na cele charytatywne

Jest oczywiste, że zakłady ubezpieczeń oczekują od swoich pracowników, aby nie angażowali się w żadną działalność, która nawet może przypominać wręczanie lub przyjmowanie łapówki. Ponieważ jednak oferowanie i przyjmowanie prezentów oraz uczestnictwo w różnych imprezach o charakterze rozrywkowym, a także sponsoring i darowizny są w pewnej formie dopuszczalne w prowadzeniu działalności biznesowej, powinny być ustanowione reguły, które pomogą pracownikom uniknąć nieświadomego przekroczenia granic i/lub zdyskredytowania niezależności zakładu ubezpieczeń w percepcji innych osób.

Zgodnie z często spotykaną praktyką wszelkie prezenty, imprezy rozrywkowe, sponsoring oraz darowizny muszą pozostawać w rozsądnych granicach co do kosztów, ilości oraz częstotliwości. Powinny być oferowane i przyjmowane w sposób jawny i przejrzysty. W przypadku wątpliwości zaleca się, aby pracownicy zwracali się o poradę do swoich przełożonych z zespołu *compliance*. Istotne jest, aby zakład ubezpieczeń posiadał własne standardy, w których zdefiniowane są limity oraz częstotliwości, jak również proces rejestracji prezentów, posiłków biznesowych oraz rozrywek. Limity, jak również zasady rejestracji, mogą być różne dla poszczególnych jednostek biznesowych, jednakże powinny precyzować wymóg, że pracownikom nie wolno przyjmować ani oferować pokrycia kosztów podróży i/lub zakwaterowania, gotówki ani ekwiwalentów pieniężnych.

Sponsoring oraz darowizny są dopuszczalne pod warunkiem, że stoi za nimi autentyczna i uzasadniona potrzeba biznesowa lub społeczna, a decyzja o zaangażowaniu się w tego rodzaju działalność została podjęta w sposób przejrzysty. Istotne jest także, aby wymóg rejestracji dotyczył również prezentów oraz udziału w imprezach rozrywkowych ofiarowanych i przyjętych w ramach sponsoringu oraz partnerstwa charytatywnego.

Insider trading

Jako *insiderzy w zakładzie ubezpieczeń* definiowani są pracownicy mogący mieć, chociażby potencjalnie, dostęp do informacji poufnych, które mogą wpływać na ceny instrumentów finansowych powiązanych z zakładem ubezpieczeń i/lub innymi spółkami giełdowymi (informacje niejawne). Pracownikom takim nie wolno wykorzystywać tych informacji w celu uzyskania osobistych korzyści, korzyści dla zakładu ubezpieczeń, klientów lub stron trzecich. Aby wspierać pracowników w przestrzeganiu tej zasady, w ramach funkcji *compliance* opracowywane są zasady i wytyczne dotyczące wykorzystywania informacji niejawnych.

Pracownicy muszą zachować ostrożność dokonując transakcji na instrumentach finansowych i powstrzymać się od takich transakcji, które mogłyby zostać uznane za niewspółmierne czy spekulacyjne. Transakcje, które można uznać za manipulujące rynkiem lub sprawiające takie wrażenie, są niedozwolone. Co więcej, rekomendowane jest, aby pracownicy, którzy są w posiadaniu informacji niejawnych:

- 1) mieli zakaz przeprowadzania transakcji finansowych powiązanych z tymi informacjami;
- 2) mieli zakaz zachęcania innych do przeprowadzania takich transakcji. Wymogi te dotyczą także kont małżonków, dzieci pozostających na utrzymaniu *insidera*, osób dzielących z nim gospodarstwo domowe oraz rachunków wspólnych;
- 3) przechowywali instrumenty finansowe zakładu ubezpieczeń na wyznaczonych rachunkach papierów wartościowych w dedykowanym banku;
- 4) przed przeprowadzeniem transakcji lub podjęciem decyzji dotyczących instrumentów finansowych zakładu ubezpieczeń uzyskali zgodę. Taka uprzednia zgoda zachowuje ważność przez ograniczony czas i wymagana jest także dla transakcji dotyczących programów opcji pracowniczych na udziały realizowanych w dedykowanych systemach operacyjnych.

Działalność zewnętrzna, interes zewnętrzny

Osoby sprawujące funkcję *compliance* powinny angażować się w przygotowywanie regulacji z zakresu działalności zewnętrznej pracowników. Zakłady ubezpieczeń na ogół zachęcają pracowników, by odgrywali aktywną rolę w swoich społecznościach. Jednak jeśli pracownicy angażują się w działalność organizacji i innych firm, np. zajmując zewnętrzne stanowiska lub mając zewnętrzne interesy, muszą oni zapewnić, że zaangażowanie takie nie będzie prowadzić nawet do pozornych konfliktów pomiędzy interesami osobistymi i zawodowymi ani w inny sposób nie zaszkodzi reputacji zakładu ubezpieczeń. Stanowisko zewnętrzne definiowane jest jako pozycja obejmowana przez pracownika poza strukturami zakładu ubezpieczeń (lub szerzej – grupy kapitałowej, której zakład jest częścią), przy czym nie ma rozróżnienia pomiędzy działalnością przynoszącą dochód a niepłatną, ani pomiędzy działalnością prowadzoną w imieniu zakładu ubezpieczeń a stanowiącą osobistą inicjatywę pracownika.

Interes zewnętrzny to interes finansowy pracownika związany z instytucją zewnętrzną wobec zakładu ubezpieczeń, który może wpłynąć na bezstronność podejmowanych przez pracownika działań zawodowych dla zakładu ubezpieczeń. W przypadku przyjęcia lub zajmowania określonych stanowisk zewnętrznych oraz wszystkich zewnętrznych interesów wprowadzany jest **mechanizm uzyskania zgody swojego przełożonego**. Uzyskanie porady z departamentu *compliance* jest na ogół wówczas obowiązkowe, zaś zewnętrzne stanowiska oraz interesy rejestrowane są centralnie. Wymagania te dotyczą:

- 1) **zewnętrznych stanowisk, na których pracownik:**
 - a) prowadzi biznes lub jednoosobową działalność gospodarczą;

- b) zajmuje dowolne stanowisko w organizacji, z którą zakład ubezpieczeń współpracuje w ramach partnerstwa lub działalności biznesowej;
- c) akceptuje kandydaturę na stanowisko w urzędzie państwowym (np. jako lokalny radny);
- d) przyjmuje płatne stanowisko w niepublicznej instytucji (np. jako audytor);
- e) przyjmuje stanowisko wiążące się z obowiązkami w zakresie księgowości (np. skarbnik, kierownik spółki);
- f) działa jako radca, doradca, ekspert lub konsultant albo wykonuje działania związane z zatrudnieniem dla organizacji, która nie stanowi części zakładu ubezpieczeń, albo ciała politycznego lub organu sądowego (lub zbliżonego), albo podobnego ciała kolegialnego lub organizacyjnego;
- g) przyjmuje członkostwo w komitetach branżowych, komisjach, forach lub panelach, jak np. członkostwo w krajowych stowarzyszeniach ubezpieczycieli, EIOPA, Chief Risk Officers Forum;
- h) jest autorem piszącym gościnnie lub komentatorem w zewnętrznych wydawnictwach;
- i) przyjmuje miejsce w zarządzie lub inne kluczowe stanowisko w niepowiązanej organizacji;
- j) obejmuje kluczowe stanowisko kierownicze lub niekierownicze (np. stanowisko dyrektora należącego lub nienależącego do zarządu, agenta lub likwidatora dowolnego podmiotu, organizacji, spółki lub korporacji, która nie jest instytucją zakładu ubezpieczeń);

2) zewnętrznych interesów w spółkach, które:

- a) prowadzą działalność na rynku finansowym;
- b) dostarczają podobne produkty i usługi klientom;
- c) są dostawcami albo klientami;
- d) mogą potencjalnie narażać reputację zakładu ubezpieczeń lub spowodować konflikt interesów.

2.3. Usługi finansowe – oferowane produkty lub usługi

Klienci stanowią punkt wyjścia wszystkich aktywności zakładu ubezpieczeń, stąd funkcja *compliance* powołana jest do dbania, aby wszystkie interakcje z klientami przebiegały według następujących **zasad współdziałania z klientem**:

- 1) dopasowanie oferty do potrzeb klientów na każdym etapie ich życia;
- 2) oferowanie klientom produktów i usług o godziwej wartości;
- 3) należyte wyjaśnianie klientom ryzyka, zysków i kosztów związanych z produktami i usługami;
- 4) regularna ocena produktów, usług oraz praktyk dystrybucyjnych;
- 5) współpraca wyłącznie z profesjonalnymi i licencjonowanymi dystrybutorami.

Produkty i usługi przygotowywane przez zakład ubezpieczeń powinny **wnosić wartość dodaną dzięki ukierunkowaniu ich na zaspokojenie potrzeb finansowych klientów oraz generowaniu zadowalającego zysku**. Funkcja *compliance* wspiera zarząd oraz funkcje biznesowe przy wyjaśnianiu kluczowych cech produktów oraz usług zrozumiałym językiem oraz przy inicjowaniu regularnych przeglądów oferowanych produktów, usług i jakości sprzedaży.

2.4. Struktura i ład biznesowy, metody prowadzenia działalności operacyjnej

Nadużycia finansowe

Nadużycia finansowe to celowe nadużycia procedur, systemu, aktywów, produktów lub usług przez osoby działające z zamiarem uzyskania w sposób podstępny lub bezprawny korzyści dla siebie lub innych. Coraz częstszą praktyką jest stosowanie polityki zerowej tolerancji w kwestiach nadużyć wewnętrznych i zewnętrznych. Specjalnie dedykowane funkcje działają w zakładach ubezpieczeń, wspierając stosowanie środków służących zwalczaniu oszustw finansowych. Pracownicy zwalczający nadużycia finansowe należą często do pionu zarządzania ryzykiem niefinansowym.

Nadużyć finansowych mogą dopuszczać się pracownicy zakładu ubezpieczeń, w tym zatrudnieni tymczasowo, zewnątrzni wykonawcy, konsultanci, klienci oraz osoby trzecie. Może to mieć wpływ na system organizacyjny, aktywa, produkty, usługi i reputację zakładu ubezpieczeń. Nadużycia to wszelkie działania noszące znamiona oszustwa, w tym celowo nierzetelna sprawozdawczość finansowa, wykroczenia przeciwko zasadom opisanym w politykach rozliczania wydatków oraz lokalnym przepisom prawa. Większość nadużyć finansowych zostaje wykryta dzięki ostrzeżeniom przed oszustwem lub raportom pochodzącym od personelu lub klientów.

Postępowanie z poufnymi informacjami

Informacje poufne to informacje, z którymi pracownicy mają do czynienia w ramach pełnienia obowiązków zawodowych. Obejmują one wszystkie dane dotyczące klientów, agentów oraz pracowników. Zabezpieczenie poufności tych informacji jest ważnym elementem codziennej pracy, a także wspólną odpowiedzialnością. Funkcja *compliance* odgrywa kluczową rolę przy definiowaniu norm regulujących obszar informacji niejawnych.

Pracownicy, występując o dostęp do poufnych informacji lub dostarczając takie informacje, korzystają z reguły nazywanej „tylko tyle, ile muszę wiedzieć”. Oznacza to, że informacja zostaje udzielona tylko pod warunkiem i w takim zakresie, w jakim jej znajomość jest konieczna do wykonania czynności ściśle związanych z realizacją obowiązków zawodowych. Zarządzaniu konfliktem interesów oraz trosce o to, by pracownicy nieświadomie nie rozpowszechniali takich informacji, służą bariery informacyjne. Od pracowników oczekuje się także podejmowania stosownych działań zapobiegających wyciekowi poufnych informacji na skutek nieostrożności, niestaranności czy niedyskrecji. Należy

zachować szczególną ostrożność podczas pracy w miejscach publicznych, takich jak restauracje, pociągi czy lotniska.

3. Usytuowanie organizacyjne funkcji *compliance* w zakładzie ubezpieczeń

3.1. Departament *compliance*

Zarząd zakładu ubezpieczeń powierza na ogół sprawowanie funkcji *compliance* specjalnie stworzonej komórce organizacyjnej, tj. departamentowi *compliance*, a osobą nadzorującą jest dyrektor (*Compliance Officer*) tego departamentu. Zadaniem departamentu *compliance* jest wspieranie zarządu i kierowników komórek organizacyjnych w zarządzaniu ryzykiem *compliance*.

3.2. Funkcja *compliance* a system zarządzania zakładem ubezpieczeń

Funkcja *compliance* jest elementem systemu kontroli wewnętrznej, będącego częścią większego systemu zarządzania funkcjonującego w oparciu o model trzech linii obrony.

- **Pierwsza linia obrony** (zarząd i kierownicy komórek organizacyjnych) ponosi bezpośrednio odpowiedzialność za bieżące zarządzanie ryzykiem, w tym monitorowanie i raportowanie ryzyka *compliance* oraz za wdrażanie zasad i polityk *compliance*. Jest odpowiedzialna także za wyniki straty.
- **Druga linia obrony** na bieżąco monitoruje skuteczność ustanowionych kontroli, identyfikuje ryzyka i potencjalne słabości w procesach. Wspomaga pierwszą linię w zarządzaniu ryzykiem *compliance*. Współpracuje z departamentem prawnym na etapie identyfikacji ryzyka *compliance*, w tym interpretacji prawa, identyfikacji obowiązków wynikających z przepisów prawa, odpowiednich wytycznych organów nadzoru, standardów biznesowych oraz procedur zakładu ubezpieczeń. Pomaga w formułowaniu strategii, polityki i struktur mających na celu zarządzanie ryzykiem *compliance*. Współpracuje z innymi komórkami organizacyjnymi wchodzącymi w skład drugiej linii obrony zapewniając odpowiednie wsparcie, w tym tzw. eskalację spraw, kiedy jest to niezbędne dla optymalizacji proporcji pomiędzy ryzykiem *compliance* a wynikającymi z niego korzyściami. Monitoruje wykonanie obowiązków wynikających z zasad i polityk *compliance* przez pierwszą linię, w tym zadań mających na celu ograniczenie ryzyka.
- **Audyt wewnętrzny, czyli tzw. trzecia linia obrony** zapewnia niezależną i obiektywną kontrolę ogólnej skuteczności wewnętrznych mechanizmów kontroli ryzyka. Zapewnia szczegółowe i konkretne rekomendacje w zakresie poprawy ładu organizacyjnego oraz struktur zarządzania ryzykiem *compliance*, ocenę adekwatności i efektywności systemu zarządzania.

Z uwagi na rolę odgrywaną w organizacji funkcja *compliance* powinna mieć zapewnioną **organizacyjną niezależność**. Instrumentem wspierającym tę

niezależność funkcyjną jest wymóg Komisji Nadzoru Finansowego określony w Zasadach Ładu Korporacyjnego, aby **dyrektor departamentu *compliance* był powoływany i odwoływany za zgodą rady nadzorczej zakładu ubezpieczeń**. W wielu zakładach ubezpieczeń dyrektorzy funkcji *compliance* traktowani są jako tzw. *Identify Staff*, co związane jest z licznymi obostrzeniami w zakresie ich powoływania oraz odwoływania, jak również zmian wynagrodzenia. W spółkach, których akcjonariat znajduje się w innych państwach, często spotykaną praktyką jest udział w wyznaczaniu celów oraz ocenie dyrektora departamentu *compliance* przez tzw. funkcję grupową *compliance*, tj. przedstawiciela funkcji *compliance* w siedzibie akcjonariusza.

Dyrektor departamentu *compliance* powinien mieć możliwość eskalacji spornych kwestii na wyższy poziom struktury zarządzania, w tym zarówno na poziomie zakładu ubezpieczeń, jak i akcjonariusza/y zakładu. Dobrą praktyką usytuowania organizacyjnego dyrektora departamentu *compliance* jest ustalenie ścieżki raportowania bezpośrednio do prezesa zarządu, z jednoczesnym prawem bezpośredniego dostępu do posiedzeń zarządu i rady nadzorczej zakładu ubezpieczeń.

Z uwagi na specyfikę biznesu ubezpieczeniowego niezależność funkcji *compliance* jest szczególnie wymagana ze względu na uczestniczenie *compliance* w tworzeniu produktów ubezpieczeniowych, procesów sprzedażowych i usługowych (w tym obsługi skarg). Jest to więc działalność znacznie wykraczająca poza koncentrowanie się na zasadach odnoszących się do prezentów, rozrywek, łapówek czy zarządzania sferą konfliktu interesów.

Częstym zagadnieniem rozważanym w zakładzie ubezpieczeń jest sposób wykonywania czynności przez *Compliance Officerów*, tj. czy *compliance* powinno blokować biznes (dawać *negative advice*), czy jedynie poprzez wskazanie ryzyka spowodować, aby biznes odstąpił od danego działania. Bez wątpienia funkcja *compliance*, jako funkcja zgodności z przepisami nie może ograniczyć się jedynie do samego wskazywania ryzyka, lecz powinna jasno określać warunki graniczne, poza które biznes nie może wykroczyć.

4. Proces zarządzania ryzykiem *compliance*

Proces zarządzania ryzykiem *compliance* składa się z pięciu podstawowych rodzajów działań, w które zaangażowani są wszyscy pracownicy.

1) Identyfikacja wymagań/ryzyka w zakresie *compliance*

Departament *compliance* „przekłada” przepisy i regulacje na obowiązki i wymagania adekwatne do prowadzonej działalności.

2) Ocena ryzyka *compliance*

Kierownicy komórek organizacyjnych i pracownicy departamentu *compliance* identyfikują i wyceniają ryzyko *compliance* związane z poszczególnymi wymogami oraz ustalają hierarchię ryzyka według przyjętej w zakładzie ubezpieczeń metodologii. W zależności od akceptowalnego przez zakład ubezpieczeń poziomu ryzyka podejmują decyzję o dalszych krokach w celu zmniejszenia ryzyka.

3) **Ograniczanie ryzyka *compliance***

Kierownicy komórek organizacyjnych opracowują i wdrażają narzędzia kontroli i ograniczania ryzyka – standardy, procedury i szkolenia w celu zminimalizowania poziomu ryzyka *compliance*.

4) **Monitorowanie ryzyka *compliance***

Kierownicy komórek organizacyjnych zapewniają bieżącą kontrolę zadań ograniczających ryzyko oraz decydują, które z zadań i narzędzi zmniejszających ryzyko wymagają przeglądu. Pracownicy departamentu *compliance* monitorują zgodność działań w zakresie obserwacji procesów z planami.

5) **Raportowanie ryzyka *compliance***

Pracownik departamentu *compliance* przedstawia raporty o ryzyku *compliance*. Pracownik ten oraz zarząd stwierdzają, czy ryzyko *compliance* przekracza przyjęty w zakładzie ubezpieczeń akceptowalny poziom. Pracownik departamentu *compliance* przedstawia okresowy raport dotyczący ryzyka *compliance*, który jest następnie przekazywany zarządowi oraz ew. funkcji *compliance* na poziomie grupowym (akcjonariatu).

5. **Compliance Chart jako narzędzie pracy funkcji *compliance***

Jednym ze spotykanych modeli używanych do holistycznego zarządzania ryzykiem *compliance* w organizacji jest *Compliance Chart* (karta *compliance*) – dokument opisujący procesy organizacji, procedury operacyjne oraz zarządzanie ryzykiem *compliance*. Jest to schemat, który wskazuje na aktualny poziom ryzyka *compliance*, przedstawia struktury, narzędzia i procesy stanowiące wytyczne do prowadzonych działań w zakresie zarządzania tym ryzykiem.

Kartę *compliance* przygotowuje departament *compliance*, a następnie zatwierdza komitet ryzyka niefinansowego (bądź równoważny komitet zarządzający ryzykiem w organizacji). W oparciu o kartę *compliance*, po zasięgnięciu opinii zarządu i wybranych kierowników komórek organizacyjnych, departament *compliance* przygotowuje plany zapewnienia zgodności z przepisami: plan monitoringów *compliance*, plan szkoleń *compliance*, plan operacyjny *compliance*.

6. **Umiejętności *Compliance Officer***

Z uwagi na zadania stawiane przed funkcją *compliance*, jej niezależnością oraz współpracą ze wszystkimi innymi funkcjami zakładu ubezpieczeń, kluczowe jest odpowiednie zidentyfikowanie i rozwijanie u pracowników niezbędnych umiejętności. Poniżej przedstawiono wybrane umiejętności, będące bardzo użytecznymi w działaniach funkcji *compliance*.

- Otwartość na słuchanie – ta kompetencja jest niezbędna przy realizowaniu funkcji wspierającej oraz funkcji zgodności wpisanych w cały proces ustalania i realizacji strategii zakładu ubezpieczeń. Umiejętność słuchania, rozumianego jako wola współdziałania z biznesem oraz identyfikowania potrzeb komercyjnych jest niezbędna dla wzajemnego zrozumie-

nia się, a przez to łatwiejszego zrozumienia doradztwa lub rekomendacji ze strony *compliance*.

- Otwartość na pomoc i zrozumienie dla biznesu.
- Pragmatyczność, a w szczególności umiejętność nie tylko „serwowania” górnolotnych i ogólnych zaleceń, ale łatwość przedstawiania konkretnych i adekwatnych rozwiązań. Dotyczy to zarówno znajomości praktyk rynkowych i to nie tylko na polskim rynku. Istotne jest także komunikowanie się prostym, nieskomplikowanym językiem, bez naleciałości żargonu języka ryzyka (np. mitygacja ryzyka). Jednym z przejawów tej umiejętności jest różnicowanie standardów w odniesieniu do różnych modeli współpracy stosowanych przez zakład ubezpieczeń.
- Rozwiązania *win-win* – szukanie kompromisowych rozwiązań.
- Asertywność – ze świadomością, jak często można ją stosować.
- Wiedza merytoryczna – znajomość zarówno produktów, jak i procesu, nie tylko posługiwanie się ogólnymi stwierdzeniami, postrzeganie przez biznes *oficera compliance* jako istotnego eksperta w *customer centricity* (tzw. *zorientowanie na klienta*), niezależnego i obiektywnego.
- Umiejętność zbierania informacji specjalistycznych z innych funkcji, np. ryzyka, aktuariatu, *pricingu* itp.

7. Relacja pomiędzy funkcją *compliance* a innymi komórkami organizacyjnymi zakładu ubezpieczeń

Pracownicy departamentu *compliance* powinni prowadzić partnerską współpracę z pracownikami pozostałych komórek organizacyjnych zakładu ubezpieczeń. Poniżej pokrótce przedstawiono istotne sfery współdziałania z wybranymi jednostkami organizacyjnymi zakładu ubezpieczeń – jest to propozycja jednego z możliwych rozwiązań organizacyjnych.

7.1. Współpraca z departamentem prawnym

Do zadań departamentu prawnego w zakładzie ubezpieczeń należy monitorowanie zmian w prawie i przekazywanie informacji o tych zmianach pracownikom, a także bieżące doradztwo i pomoc departamentowi *compliance* w zakresie identyfikacji obowiązków wynikających z przepisów prawa. Departamenty współpracują także w zakresie kontaktów z organami nadzoru.

7.2. Współpraca z departamentem zarządzania ryzykiem niefinansowym

Do zadań departamentu zarządzania ryzykiem niefinansowym należy monitorowanie poprawności kontroli w kluczowych procesach pod kątem ryzyka operacyjnego, doradzanie w sprawach dotyczących oceny ryzyka, prowadzenie i monitorowanie rejestru kluczowych ryzyk oraz obsługa incydentów. Departament *compliance* współpracuje z departamentem zarządzania ryzykiem niefinansowym przy wycenie ryzyka, przygotowywaniu kwartalnego raportu ryzyka niefinansowego w organizacji (*Non-financial Risk Dashboard* (NFRD), czyli tzw. Raport ryzyk niefinansowych) oraz zarządzaniu incydentami, przygotowaniu planu monitoringów (tak, aby nie pokrywały się

zakresowo). Ważna jest również współpraca przy organizacji i prowadzeniu warsztatów ryzyka.

7.3. Współpraca z departamentem produktowym

Analizując obecne otoczenie regulacyjne na szczególną uwagę zasługuje współpraca funkcji *compliance* z komórką odpowiedzialną za tworzenie oraz modyfikację oferty produktowej. Istotne jest, aby przedstawiciel *compliance* blisko współpracował z menedżerami produktowymi już od wstępnej fazy rozwoju produktu. Funkcja *compliance* wspiera zespół tworzący produkty ubezpieczeniowe we wdrażaniu regulacji wydawanych przez regulatorów. W tym zakresie należy wskazać w szczególności wdrożenie i monitorowanie zgodności z rekomendacjami wydanymi w 2016 r. przez Komisję Nadzoru Finansowego (tj. Rekomendacje dotyczące systemu zarządzania produktem oraz Rekomendacje dotyczące badania adekwatności produktu).

7.4. Współpraca z funkcją odpowiedzialną za obszar danych osobowych

Dotychczas funkcja odpowiedzialna za zgodność z prawem z zakresu danych osobowych umieszczana była w ramach funkcji *compliance*. Wydaje się, że w związku z wejściem w życie rozporządzenia RODO⁵ istotne jest utrzymanie tej funkcji w departamencie *compliance*, w szczególności dla odróżnienia od specjalisty ds. jakości danych, która to funkcja wynika z Wytycznych dotyczących zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego.

Kluczowe pozostaje także powiązanie tej funkcji z troską o klienta i koniecznością zapewnienia zgodności z prawem, a także w procesach digitalizacji i rozwoju FinTech.

7.5. Współpraca z funkcją MLRO

Istnieje tendencja umieszczania funkcji MLRO w tzw. pierwszej linii w operacjach, zaś *compliance* ze szczególną uwagą monitoruje zgodność w tym obszarze. Bardzo istotna jest tu duża atencja grup kapitałowych do identyfikacji klienta *up front* (szczególnie prowadzących działalność biznesową z zastosowaniem regulacji amerykańskich, które w tym obszarze są bardzo restrykcyjne).

8. Udział funkcji *compliance* w komitetach ryzyka

Departament *compliance* poprzez uczestnictwo w komitetach ryzyka w sposób aktywny identyfikuje, dokumentuje i ocenia ryzyko *compliance* związane z działalnością operacyjną zakładu ubezpieczeń, oferowanymi i projektowanymi produktami, działalnością agentów ubezpieczeniowych i osób wykonujących czynności agencyjne. Często praktyką jest, aby dyrektor departamentu *comp-*

⁵ Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (Dz. Urz. UE L 119 z 4.05.2016).

liance lub wyznaczony przez niego pracownik był członkiem następujących komitetów zakładu ubezpieczeń: komitetu ds. ryzyka niefinansowego, komitetu ds. ryzyka produktowego i portfelowego, komitetu ds. jakości sprzedaży, komitetu kryzysowego.

9. Relacja z organem nadzoru

Zakład ubezpieczeń prowadzi działalność na regulowanym rynku finansowym, gdzie większość działań jest nadzorowanych przez Komisję Nadzoru Finansowego (KNF). KNF jest uprawniona do żądania od zakładu ubezpieczeń przygotowania informacji i materiałów oraz przeprowadzania kontroli w każdym czasie i zakresie, związanych z działalnością zakładu ubezpieczeń. Na podstawie przygotowanych przez zakład ubezpieczeń informacji i materiałów KNF podejmuje decyzje nadzorcze i inne czynności w ramach realizowanej polityki nadzoru, w tym bezpośrednio dotyczące ubezpieczyciela.

Podobnymi uprawnieniami dysponują również inne organy administracji publicznej nadzorujące działalność towarzystw ubezpieczeniowych, m.in. Urząd Ochrony Konkurencji i Konsumentów i Generalny Inspektor Ochrony Danych Osobowych.

Istotne jest, by wszystkie informacje i materiały przekazywane na żądanie wymienionych organów były przygotowane rzetelnie i zgodnie ze stanem faktycznym. Udzielenie informacji z naruszeniem terminu, informacji nieprawdziwej, nierzetelnej, czy wprowadzającej w błąd może skutkować konsekwencjami natury administracyjnej i finansowej. Właściwe relacje z organem nadzoru powinny być istotnym elementem polityki zakładu ubezpieczeń i wyrazem realizacji wartości, którymi kieruje się zakład w wykonywanej działalności.

Szczególnym przykładem współdziałania z organem nadzoru jest pozyskiwanie informacji, materiałów i wyjaśnień w trybie bezpośredniej kontroli w siedzibie zakładu ubezpieczeń. Sytuacją niedopuszczalną jest przedkładanie informacji nieprawdziwych lub mogących wprowadzać w błąd, niezwyfikowanych, niekompletnych, zawierających błędy materiałów czy informacji lub opóźnienia w ich przekazywaniu, o ile nie uzgodniono dodatkowego terminu. Przygotowywane informacje, materiały i wyjaśnienia przed ich przekazaniem powinny być odpowiednio zweryfikowane przez np. pracowników funkcji *compliance*. Istotne jest, aby każdy pracownik zaangażowany w czynności z udziałem organu nadzoru był świadomy, że reprezentuje zakład ubezpieczeń. Przez profesjonalną, rzetelną i uczciwą postawę w stosunku do organów nadzoru buduje się swój wizerunek na rynku.

10. Podsumowanie

W ocenie autora niniejszego opracowania w obecnej sytuacji należy podkreślić rosnące znaczenie funkcji *compliance* w zakładach ubezpieczeń, tak jak i w innych instytucjach finansowych. Obok niezmiernie ważnej roli *compliance* w procesie zapewnienia działania jednostek biznesowych zgodnie z tzw. zasadą uczciwości (*integrity*), *compliance* musi angażować się w proces współtworzenia oferty produktowej oraz procesów sprzedażowych.

Dodatkowo należy zwrócić uwagę na niezwykle istotny aspekt odpowiedzialności za relację z regulatorami. Przy czym chodzi tu nie tylko o zapewnienie zgodności z przepisami prawa, ale i z rekomendacjami regulatorów. Wszystko to prowadzi do tego, że specjalista ds. *compliance* musi uwzględniać coraz szerszy kontekst biznesowy i regulacyjny, w którym przychodzi mu działać.

Poglądy wyrażone w artykule są poglądami osobistymi autora i nie wyrażają oficjalnego stanowiska instytucji, w której jest zatrudniony.

Karol Rajewski

*Dyrektor Departamentu Prawnego Urzędu Komisji Nadzoru Finansowego
– ekspert compliance na rynku ubezpieczeniowo-finansowym*

Bibliografia

- Borowa M.B., „Program compliance – przepis na sukces. Jakie wymagania powinny być spełnione z praktycznego punktu widzenia?”, w: Makowicz B. (red.) „Metody efektywnego kształtowania systemów compliance”, dodatek do Monitora Prawniczego 2013, nr 23.
- Borowa M.B., R. Preusche, „Fostering regulatory and fair conduct of business-a compliance programme basics”, *Controlling* 2014, nr 32.
- Bockelmann F., „Compliance and operative risks-Reporting in the company”, *Controlling* 2014, nr 32.
- Gołębiowski P., „Prawne aspekty funkcji compliance”, *Prawo Bankowe* 2008, nr 9.
- Haase M., „Officer compliance jako zawód”, dodatek do Monitora Prawniczego 2013, nr 23.
- Isenberg D., „Przedsiębiorcy i kult porażki”, *Harvard Business Review*, luty 2012.
- Jagura B., B. Makowicz, „Prywatne dochodzenie w przedsiębiorstwie metodą skutecznego systemu compliance”, w: Makowicz B. (red.), „Metody efektywnego kształtowania systemów compliance”, dodatek do Monitora Prawniczego 2013, nr 23.
- Jagura B., T. Szarowicz, „Prawne podstawy systemów zarządzania compliance w prawie niemieckim i polskim”, *Controlling*, marzec–kwiecień 2014, nr 32.
- Ligęza D., „Ryzyko compliance”, *Problemy Prawa i Administracji* 2010, nr 1.
- Makowicz B., „Compliance w przedsiębiorstwie”, Wolters Kluwer, Warszawa 2011.
- Makowicz B., „Compliance dla wszystkich, czyli korzyści płynące z systemu zarządzania zgodnością w przedsiębiorstwie”, *Controlling* 2014, nr 32.
- Meckenstock C., „Struktura i wdrażanie systemów compliance – wprowadzenie praktyczne”, dodatek do Monitora Prawniczego 2013, nr 23.
- Mikes A., „Nowa koncepcja zarządzania ryzykiem”, *Harvard Business Review*, marzec 2013 r.
- Piesik L., „Wspomagająca technologia”, *Gazeta Bankowa* 2008, nr 21.
- Rajewski K., Jak daleko powinno sięgać compliance – czy powinno pełnić funkcję doradczą czy kontrolną? Kilka uwag z branży finansowej, dodatek do Monitora Prawniczego 2013, nr 23.
- Rajewski K., „Wyzwania i bariery w procesie digitalizacji”, *Compliance – Magazyn Fachowy Instytutu Compliance*, czerwiec 2017, nr 2.
- Rastegar F., „Wadliwy produkt i wadliwa akcja serwisowa”, *Harvard Business Review*, luty 2012 r.
- Staniec I., „Perspektywy rozwoju compliance”, *Controlling* 2014, nr 32.

- Mrozowska B., A. Wnęk, „Funkcja *compliance* w zakładzie ubezpieczeń”, *Prawo Asekuracyjne* 2016, nr 1.
- Szczepański M., „Wdrażanie systemu *compliance* w polskiej rzeczywistości”, w: Makowicz B. (red.) „Metody efektywnego kształtowania systemów *compliance*”, dodatek do *Monitora Prawniczego* 2013, nr 23.
- Ziomko R., „Polskie firmy coraz lepiej zarządzają ryzykiem”, *Harvard Business Review*, luty 2012 r.

The Compliance Function in the Organizational Structure of an Insurance Undertakings – Challenges and Practical Aspects

Management of company's compliance with broadly understood legal regulations and other standards, known as compliance, is playing an increasingly important role in insurance undertakings. The primary purpose of this function, being one of the key features of the risk management system and an element of internal audit, is the development of such an organization of the insurance undertaking and the cooperation of all employees to ensure that business processes comply with the legal regulations, recommendations and guidelines of the regulators, strategy as well as declared ethical values.

The author presents selected issues crucial for compliance risk management in an insurance undertaking. Moreover, he discusses the relationship between the compliance function and other organizational units and the supervisory authority. What is presented within the framework of the article is only the structure of tasks facing compliance in a changing market situation. Certain aspects should obviously be developed in detail, which would require individual articles according to the author.

Keywords: compliance, insurance company management system, key functions, internal audit, risk management, compliance risk management.