Vademecum specjalisty ds. compliance + wzory do pobrania

Fragment

Michał Kaczmarski

Rozdział I. Funkcja specjalisty ds. compliance oraz jej usytuowanie w modelu trzech linii obrony

1. Uwagi wstępne

Już od czasów starożytnych Rzymian znane jest twierdzenie, że prowadzenie działalności zarobkowej wiąże się z podejmowaniem ryzyka (łac. *commodum eius esse debet*, *cuius est periculum*). Skoro zatem PrPrzed wskazuje, że działalnością gospodarczą jest zorganizowana działalność zarobkowa (art. 3 PrPrzed), możemy śmiało założyć, że jej wykonywanie wiąże się z podejmowaniem ryzyka.

Współcześnie jednak ryzyko to posiada o wiele szerszy kontekst niż w czasach rzymskich, gdzie sprowadzało się, co do zasady, do skutków na płaszczyźnie cywilnoprawnej. Działalność gospodarcza w XXI w. jest obwarowana szerokim spektrum ograniczeń i obowiązków, dlatego sprawne poruszanie się w gąszczu regulacji prawnych wymaga w przedsiębiorstwach profesjonalnego wsparcia, bo przecież każdy ma obowiązek przestrzegania prawa Rzeczypospolitej Polskiej (art. 83 Konstytucji RP) – przedsiębiorcy nawet bardziej, ponieważ należytą staranność w zakresie prowadzonej działalności gospodarczej określa się przy uwzględnieniu zawodowego charakteru tej działalności (art. 355 § 2 KC). Skutki naruszenia regulacji prawnych mogą się natomiast wiązać z dotkliwą odpowiedzialnością natury administracyjnej, karnej oraz cywilnej.

Funkcjonowanie w złożonym środowisku regulacyjnym wymaga przy tym połączenia wielu kompetencji zarówno merytorycznych, jak i tzw. miękkich, dotyczących zarządzania relacjami z ludźmi w złożonych strukturach korporacyjnych, nierzadko rozproszonych geograficznie, wielokulturowych i funkcjonujących w trybie ciągłym. W wielu dzisiejszych podmiotach korporacyjnych działalność gospodarcza jest prowadzona na wszystkich kontynentach, a w związku z tym przez całą dobę.

Co więcej, współczesne korporacje międzynarodowe potrafią generować przychody ze sprzedaży, przewyższające PKB krajów średniej wielkości na świecie, posiadają zatem kapitały i aktywa, które pozwalają na wywieranie wpływu, nie tylko zresztą na osoby tam zatrudnione, lecz także całe społeczeństwa, a niekiedy również państwa.

Przykład

Spółka Apple w sprawozdaniu finansowym za rok obrotowy kończący się 30.9.2023 r. wskazuje na całkowitą sprzedaż netto na poziomie 383 mld dolarów amerykańskich[1] (383×10^9). Dla porównania, Dania w 2022 r. wygenerowała PKB na poziomie 400 mld dolarów amerykańskich (400×10^9)[2], a Polska w tym samym roku zarejestrowała PKB na poziomie 688 mld dolarów amerykańskich (688×10^9)[3].

Wynika z tego, że sprzedaż netto spółki Apple (tylko jedno przedsiębiorstwo) generuje przychody na poziomie 55% produktu krajowego brutto Polski i podobnym poziomie jak Dania.

Dodać możemy, że Apple wygenerował wspomniany przychód ze sprzedaży netto zatrudniając 161 tys. pracowników[4], podczas gdy na PKB Danii pracowało 6 mln obywateli, a w Polsce prawie 37 mln.

Osobą, która ma za zadanie wspierać środowisko korporacyjne w realizacji jego celów operacyjnych (biznesowych), ale z uwzględnieniem ograniczeń wynikających z przepisów prawa oraz praktyki rynkowej w interpretacji tych przepisów, jest natomiast **specjalista ds. compliance**.

Kolejne podrozdziały stanowią wprowadzenie do usytuowania specjalisty ds. compliance w strukturze korporacyjnej – zarówno w wymiarze operacyjnym, jak i kompetencyjnym. A wszystko to na tle orzecznictwa i piśmiennictwa odnoszącego się do problematyki compliance, czyli zgodności działań operacyjnych przedsiębiorstw z regulacjami prawnymi znajdującymi zastosowanie do konkretnego przedsiębiorstwa w konkretnym kontekście biznesowym jego działalności.

2. Business compliance jako obszar zainteresowania specjalisty ds. compliance

2.1. Wielowymiarowy charakter wymogów business compliance

Na potrzeby niniejszego opracowania „business compliance" zdefiniujemy jako wykonywanie działalności gospodarczej w sposób zgodny z pewnymi „zasadami gry" – com-

[1] Apple Inc., Annual Report Pursuant to Section 13 Or 15(D) of the Securities Exchange Act of 1934, For the fiscal year ended September 30, 2023, źródło: https://s2.q4cdn.com/470004039/files/doc_earnings/2023/q4/filing/_10-K-Q4-2023-As-Filed.pdf (dostęp: 25.5.2024 r.), s. 24.

[2] Dane Banku Światowego, https://data.worldbank.org/indicator/NY.GDP.MKTP.CD?locations=DK (dostęp: 25.5.2024 r.).

[3] Dane Banku Światowego, https://data.worldbank.org/indicator/NY.GDP.MKTP.CD?locations=PL (dostęp: 25.5.2024 r.).

[4] Apple Inc., Annual Report..., s. 7.

pliance to przecież nic innego jak zachowanie zgodności. Zgodność ta obejmuje przy tym 3 wymiary:

1) przedmiotowy,
2) operacyjny,
3) podmiotowy.

2.1.1. Wymiar przedmiotowy

W wymiarze przedmiotowym standardy zgodności są wyznaczane, co do zasady, przez przepisy prawa, które posługują się jednak często klauzulami generalnymi (np. należyta staranność lub określenia, takie jak „słuszne interesy" czy „dobre obyczaje"), które w praktyce rynkowej wymagają doprecyzowania na poziomie operacyjnym, w szczególności przez tzw. dobre praktyki rynkowe, rekomendacje organów nadzoru, praktykę orzeczniczą sądów, pisma urzędowe organów administracji oraz procedury wewnętrzne funkcjonujące u konkretnego przedsiębiorcy.

Przykładem przepisu zawierającego klauzule generalne może być art. 9 PrPrzed, który stanowi, że: „Przedsiębiorca wykonuje działalność gospodarczą zgodnie z zasadami uczciwej konkurencji, poszanowania dobrych obyczajów oraz słusznych interesów innych przedsiębiorców i konsumentów, a także poszanowania oraz ochrony praw i wolności człowieka".

Wspomniane klauzule generalne znajdują swoje doprecyzowanie w dalszych przepisach prawa lub orzecznictwie sądów, a także kodeksach dobrych praktyk rynkowych czy stanowiskach organów nadzoru. Oczywiście ich podmiotowa i przedmiotowa subsumpcja, czyli odnalezienie normy postępowania właściwej dla danego stanu faktycznego, odbywa się już indywidualnie dla konkretnego przedsiębiorcy i kontekstu biznesowego, w którym funkcjonuje.

Za nieprzestrzeganie zasad grozi zazwyczaj kara, która ma za zadanie, z jednej strony, przywrócić stan pożądany przez „zasady gry" obowiązujące w obrocie gospodarczym, a z drugiej – działać odstraszająco na ewentualnych naśladowców podmiotów łamiących zasady, w ramach prewencji ogólnej.

Warto w tym miejscu wspomnieć, że w ramach prowadzonej działalności gospodarczej obowiązują zarówno zasady dotyczące wszystkich przedsiębiorców, jak np. zasady wynikające z obowiązku ponoszenia danin publicznych w postaci podatku dochodowego czy należnego podatku VAT, jak i zasady szczególne, odnoszące się jedynie do pewnych rodzajów działalności gospodarczej, zazwyczaj z obszaru tzw. działalności regulowanej. Chodzi tutaj o pewne rodzaje działalności gospodarczej wymagające dla jej wykonywania uzyskania uprzedniego zezwolenia, koncesji lub wpisu do właściwego rejestru. Te ostatnie działalności są zazwyczaj obwarowane dodatkowymi obowiązkami. Dzieje się tak np. w przypadku działalności gospodarczej związanej z udziałem w legalnym łańcuchu wytwarzania i dystrybucji leków lub wyrobów medycznych albo w przypadku działalności bankowej, maklerskiej lub inwestycyjnej na zlecenie. Uczestnicy legalnego łańcucha wytwarzania i dystrybucji leków będą zobligowani do stosowania przepisów PrFarm i jego aktów wykonawczych, a w drugim przypadku – PrBank, ObrInstrFinU lub FundInwU wraz z ich przepisami wykonawczymi. Dodatkowo w odniesieniu do rynku

wytwarzania i obrotu lekami istotne znaczenie mają także stanowiska, wytyczne i interpretacje Głównego Inspektora Farmaceutycznego lub Urzędu Rejestracji Produktów Leczniczych, Wyrobów Medycznych i Produktów Biobójczych albo Ministerstwa Zdrowia, a także orzecznictwo sądów administracyjnych. W odniesieniu do rynku usług finansowych nie możemy zapominać zwłaszcza o stanowiskach i rekomendacjach UKNF lub zapisach TerroryzmU. Ponadto, z uwagi na obecność Polski w strukturach UE, wszystkie podmioty uczestniczące w obrocie gospodarczym, a w szczególności uczestnicy rynku regulowanego, są zobligowani do stosowania regulacji UE, a w szczególności rozporządzeń UE, które na podstawie art. 288 TFUE mają zasięg ogólny, są wiążące w całości i stosowane bezpośrednio, co do zasady, we wszystkich państwach członkowskich UE.

Rysunek 1. Compliance u ujęciu przedmiotowym (podsumowanie graficzne)

Przykład

Krajowa firma farmaceutyczna ABC w ramach prowadzonej działalności gospodarczej polegającej – w uproszczeniu – na wytwarzaniu i dystrybucji leków musi zazwyczaj spełnić wiele wymogów regulacyjnych odnoszących się do obszarów:

1) badań klinicznych;
2) uzyskania pozwolenia na dopuszczenie do obrotu;
3) wytwarzania;
4) reklamy i promocji;
5) uzyskania refundacji (w przypadku kosztownych terapii lekowych to często jedyny sposób, aby lek mógł dotrzeć do pacjenta);
6) dystrybucji;
7) przetwarzania danych osobowych, w tym danych wrażliwych na etapie badań klinicznych (tj. danych dotyczących stanu zdrowia pacjentów uczestniczących w badaniach).

W celu spełniania wymogów compliance spółka ABC musi zapoznać się i wdrożyć środowisko kontroli, które spełni wymogi:

1) przepisów prawa krajowego, rozporządzeń Parlamentu Europejskiego i Rady oraz rozporządzeń delegowanych Komisji Europejskiej, np.: BadKliniczneU, PrFarm, RODO, rozporządzenia 2016/161, czy dobrych praktyk w zakresie badań klinicznych (GCP), wytwarzania (DPW) lub dystrybucji (DPD) leków, a także
2) branżowych kodeksów dobrych praktyk, np.: Związku Pracodawców Innowacyjnych Firm Farmaceutycznych INFARMA[5]. Kodeksy dobrych praktyk doprecyzowują zresztą często, niekiedy nazbyt blankietowe, przepisy ustaw i rozporządzeń, przez co sprawiają, że norma blankietowa dla firmy członkowskiej organizacji branżowej zostaje wypełniona treścią.

Niezastosowanie się do wymogów compliance może wiązać się z dotkliwymi konsekwencjami natury prawnej lub utratą reputacji.

2.1.2. Wymiar operacyjny

W wymiarze operacyjnym zachowanie zgodności to w praktyce stworzenie w organizacji gospodarczej środowiska kontroli wyrażonego w ramach tzw. programu compliance, czyli – najprościej rzecz ujmując – ekosystemu korporacyjnego dla przestrzegania standardów compliance w ujęciu przedmiotowym (omówionym wyżej), obejmującego w szczególności:

1) **bieżącą ocenę ekspozycji na ryzyko** naruszenia reguł gry rynkowej, zwłaszcza w odniesieniu do przepisów powszechnie obowiązującego prawa wyposażonych w normy sankcjonujące o charakterze karnoprawnym lub administracyjnym;
2) **wdrożenie środowiska kontroli** ograniczającego ryzyko naruszenia zasad compliance w znaczeniu przedmiotowym;
3) **opracowanie procedur** wewnętrznych i instrukcji stanowiskowych pozwalających na stosowanie mechanizmów kontrolnych przez pracowników i podwykonawców w praktyce, a także **szkolenia** z praktycznego stosowania tych procedur;
4) tzw. **monitoring compliance**, czyli bieżącą weryfikację zgodności działań operacyjnych przedsiębiorstwa z procedurami wewnętrznymi i instrukcjami, w tym w odniesieniu do realizacji szkoleń ze stosowania ww. procedur i instrukcji. Monitoring compliance obejmuje również zapewnienie kanałów komunikacji z pracownikami i podwykonawcami umożliwiających komunikację wewnętrzną w organizacji (tzw. kultura *speak-up*) oraz zgłaszanie zaobserwowanych nieprawidłowości (sygnaliści), a także wsparcie merytoryczne w realizacji procedur wewnętrznych i instrukcji oraz przyjmowanie informacji zwrotnej (tzw. *feedback*) w odniesieniu do elementów środowiska kontroli, których realizacja sprawia problemy lub budzi wątpliwości;
5) reakcję na **incydenty tzw. non-compliance**, czyli działań naruszających procedury wewnętrzne i instrukcje stanowiskowe, a niekiedy również przepisy powszechnie obowiązującego prawa. W tym kontekście konieczne jest wdrożenie procedur obejmujących:
   a) model wewnętrznego postępowania wyjaśniającego,
   b) sposób i treść komunikacji wobec pracowników i podwykonawców konsekwencji naruszenia przez nich procedur wewnętrznych lub prawa. Fakt istnie-

[5] Zob. https://www.infarma.pl/etyka/kodeks-dobrych-praktyk/ (dostęp: 26.5.2024 r.).

nia regulacji w tym zakresie, np. w KP czy KC nie wystarczy, jeśli pracownicy lub podwykonawcy nie mają świadomości tych regulacji lub intencji ich stosowania po stronie pracodawcy lub zleceniodawcy,

c) zasady zapewnienia ochrony osobom zgłaszającym nieprawidłowości, w tym dostatecznie odstraszające konsekwencje wobec osób, które stosują wobec tzw. sygnalistów działania odwetowe.

W przypadku, gdy w ramach badania zidentyfikowanego incydentu non-compliance okaże się, że doszło do naruszenia procedur wewnętrznych lub prawa lub w inny sposób zostanie zdiagnozowana luka w środowisku kontroli, konieczne będzie **podjęcie działań naprawczych**;

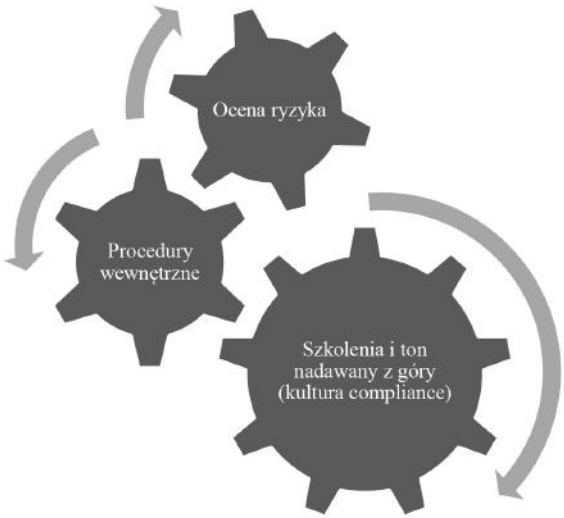
6) **ton nadawany z góry** oraz budowanie **kultury compliance**, czyli komunikacja wspierająca ze strony kierownictwa. Za przykład niech posłużą znane z globalnych korporacji hasła typu:
   a) „*lead by example*", czyli bądź liderem, dając przykład własnej postawy, którą inni chcieliby naśladować. To ostatnie jest zresztą równie ważne jak pierwsze, należy zatem zadbać zarówno o treść, jak i atrakcyjną formę przekazu, tak aby zyskać naśladowców wśród jego odbiorców. I najważniejsze, musimy w ogóle do nich dotrzeć. Wybory parlamentarne w Polsce w 2023 r. pokazały zresztą, jak potężnym medium wyborczym jest Internet, a w odniesieniu do niektórych partii politycznych – w szczególności chińska platforma TikTok,
   b) „*walk the talk*", czyli postępuj w taki sposób, jak mówisz, że chciałbyś, żeby postępowali inni. Będąc liderem organizacji, musisz zatem sam lub sama stanowić forpocztę własnych słów i pokazać innym, że istnieje jedność pomiędzy deklaracjami i działaniem następującym po deklaracjach. W sytuacji gdy brak dowodu spójnego z deklaracjami działania po stronie kierownictwa wyższego szczebla, „w korytarzach" korporacji usłyszeć można, że to tylko „takie gadanie", a w firmie są „równi i równiejsi".

Bez zapewnienia funkcjonującego programu compliance trudno wyobrazić sobie możliwość zapewnienia zgodności z wymogami regulacyjnymi, a to właśnie naruszenie tych wymogów może się wiązać z:

1) dotkliwymi karami administracyjnymi dla przedsiębiorcy, a niekiedy także osób zarządzających przedsiębiorstwem;
2) korporacyjną odpowiedzialnością karną;
3) indywidualną odpowiedzialnością karną pracowników lub podwykonawców będących osobami fizycznymi;
4) utratą reputacji;
5) utratą najbardziej kompetentnych pracowników, najlepszych dostawców lub klientów, którzy odejdą w obawie przed uszczerbkiem dla własnej reputacji.

Warto również pamiętać, że skuteczny program compliance jest systemem naczyń połączonych, co oznacza, że jego elementy są **wzajemnie zależne i komplementarne**.

Rysunek 2. Program compliance, czyli system naczyń połączonych



Bez uprzedniej i na bieżąco aktualizowanej oceny ryzyka i stworzenia środowiska kontroli procedury nie będą adresowały wrażliwych obszarów działalności firmy. Podobnie dobrze zaprojektowane środowisko kontroli nie będzie funkcjonować bez instrukcji obsługi w postaci procedur wewnętrznych oraz szkoleń dla pracowników z obsługi tego środowiska.

Dodatkowo nawet procedury i szkolenia nie uchronią nas przed nadużyciami i ryzykiem prawnym, jeżeli operatorzy tych procedur, czyli nasi pracownicy, będą dostrzegać, że compliance jest tylko hasłem, a nie przedmiotem codziennej troski ze strony kierownictwa firmy.

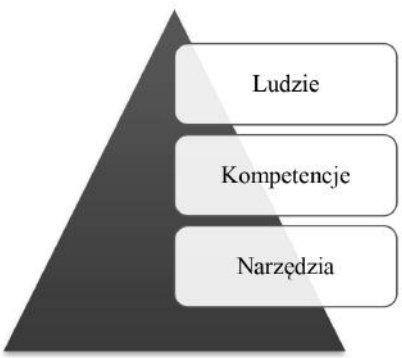
2.1.3. Wymiar podmiotowy

W wymiarze podmiotowym business compliance oznacza zapewnienie w organizacji obecności osoby lub osób odpowiedzialnych za koordynację wdrożenia programu compliance i dbałość o jego bieżącą aktualizację. W praktyce na początku wdrożenia programu compliance bywa, że komórka compliance jest bytem jednoosobowym, a nawet etatem łączonym, nierzadko w ramach tandemu, np. z działem prawnym, finansowym lub – np. w firmach farmaceutycznych – z tzw. działem regulatory, czyli odpowiedzialnym m.in. za rejestrację leków i badań klinicznych oraz poprawność merytoryczno-językową komunikacji dotyczącej leków, zarówno w wymiarze promocji, jak i pozapromocyjnym. Oczywiście z czasem, zależnie od skali działalności przedsiębiorstwa oraz jego usytuowania w środowisku regulacyjnym, tj. sektor regulowany czy też nie, komórka compliance ulega wyodrębnieniu do roli niezależnego elementu struktur korporacyjnych.

Niezależnie od ich usytuowania w strukturze organizacyjnej kluczowe jest, aby osoby odpowiedzialne za zapewnienie compliance posiadały wiedzę w zakresie przedmiotowego

oraz operacyjnego aspektu programu compliance, a jeśli jej nie posiadają, należy zapewnić im adekwatne szkolenie w tym zakresie. Komórka compliance jest bowiem tą jednostką, która stanowi pomost pomiędzy realizacją celów biznesowych oraz środowiskiem ryzyka i kontroli, które towarzyszą realizacji tych celów. Dodatkowo, z uwagi na konieczność zapewnienia ścieżki audytu dla prowadzonych przez compliance działań operacyjnych, konieczne jest zapewnienie komórce compliance dostępu do danych i informacji oraz narzędzi wspierających przetwarzanie tych danych w zakresie niezbędnym do realizacji jej zadań operacyjnych w ramach tzw. drugiej linii obrony, której emanacją jest właśnie komórka compliance w ujęciu podmiotowym.

Rysunek 3. Compliance w wymiarze podmiotowym



Nie każdy model funkcjonowania komórki compliance jest jednak akceptowalny merytorycznie.

Przykład

Przykładowo trudno uzasadnić połączenie roli specjalisty ds. compliance z rolą kierownika sprzedaży, a to z tego powodu, że pomiędzy tymi rolami występuje oczywisty konflikt interesów.

Osoba odpowiedzialna za sprzedaż pozostaje pod presją realizacji wyników i z tego jest rozliczana.

Compliance natomiast stoi ma straży działania w zgodzie z procedurami i prawem, nawet jeśli oznacza to odstąpienie od ubiegania się o konkretne zlecenie, np. z uwagi na presję zamawiającego na podjęcie czynności o charakterze korupcyjnym lub zakupu towaru po niespotykanie atrakcyjnej cenie, np. w związku z faktem, że potencjalny dostawca objęty jest sankcjami gospodarczymi albo w domenie publicznej pojawiają się informacje o jego uwikłaniu w przestępstwa o charakterze karuzeli VAT.

W większych organizacjach – np. międzynarodowych instytucjach finansowych lub globalnych firmach farmaceutycznych – osoby funkcjonujące w roli specjalistów ds. compliance (formalnie często, jako członkowie zarządów w grupie spółek, dyrektorzy lub kierownicy/menedżerowie) mogą kierować całymi zespołami osób, a dodatkowo korzystają ze wsparcia outsourcingu w realizacji określonych czynności w ramach realizacji programu compliance.

2.2. Compliance w kontekście pomiaru ryzyka i apetytu na ryzyko

Wdrożenie efektywnego programu compliance, z uwagi na jego wielopłaszczyznowość (ludzie, technologia oraz środowisko kontroli) oraz mocne osadzenie w środowisku regulacyjnym, może stanowić wyzwanie operacyjne dla wielu organizacji gospodarczych. Wyzwanie po stronie regulacyjnej wynika w dużej mierze z faktu, że skuteczność programu compliance jest zależna od zdiagnozowania środowiska ryzyka, w którym funkcjonuje konkretny podmiot gospodarczy.

Diagnoza ta ma przy tym charakter dynamiczny, ponieważ **środowisko ryzyka jest zmienne w czasie**, co wynika w szczególności z:

1) **ciągłych zmian** w środowisku regulacyjnym, w ostatnim czasie np. sygnaliści, ESG i przeciwdziałanie praniu pieniędzy, zmiany w przepisach podatkowych spowodowane wprowadzeniem „Polskiego Ładu";
2) **ewolucji modeli biznesowych** stosowanych przez przedsiębiorców, np. kanały dystrybucji, modele dystrybucji, zasięg geograficzny, struktury korporacyjne itp.;
3) **otoczenia politycznego i biznesowego** przedsiębiorców, czego w ostatnich latach doświadczamy w szczególności w związku z niedawną pandemią COVID-19 oraz konfliktem zbrojnym w Ukrainie.

Dynamika zmian w środowisku ryzyka wymaga zatem ciągłej adaptacji, ponieważ brak dostosowania do zmieniającego się środowiska regulacyjnego oraz biznesowego może dużo kosztować. Koszt ten przy tym nie ogranicza się jedynie do kar finansowych, ale także do ryzyka utraty przychodów, a w efekcie również zaufania ze strony interesariuszy, zwłaszcza akcjonariuszy i najbardziej kompetentnych pracowników. W przeszłości firmy, takie jak Nokia czy Kodak, nie dostosowały się do zmieniających się warunków na rynku i utraciły swoją dominację wśród klientów. Z perspektywy regulacyjnej niezareagowanie na zmieniające się warunki regulacyjne kosztowały firmę Siemens AG wiele miliardów dolarów wynikających z kar finansowych oraz koniecznych inwestycji w dostosowanie programu compliance do standardu wymaganego przez przepisy prawa. O tym ostatnim, w kontekście zarządzania zmianą w środowisku regulacyjnym, więcej w dalszej części niniejszego rozdziału.

Zarządzanie ryzykiem niedostosowania do wymogów zmieniającego się środowiska korporacyjnego, jak większość elementów programu compliance, jest zadaniem cyklicznym. Obejmuje zazwyczaj wstępną diagnozę środowiska ryzyka, określenie apetytu na ryzyko, a w razie konieczności wdrożenie środowiska kontroli odpowiadającego apetytowi na ryzyko oraz bieżące monitorowanie zmian w środowisku ryzyka, w celu uchwycenia zdarzeń o istotnym znaczeniu, które mogą wymagać zmian w środowisku kontroli.

2.2.1. Wstępna diagnoza środowiska kontroli

Wstępna diagnoza środowiska kontroli to nic innego jak zgromadzenie danych wejściowych. Dane wejściowe to suma diagnozy ekspozycji na ryzyko regulacyjne w konkretnej organizacji gospodarczej oraz oceny skuteczności zastanego w tej organizacji środowi-

ska kontroli na tle indywidualnego apetytu na ryzyko, co można wyrazić poniższym wzorem[6]:

Dane wejściowe = (wstępna diagnoza ryzyka + dostępne środowisko kontroli) × apetyt na ryzyko

Jeśli z jakiegokolwiek powodu zabraknie w środowisku kontroli mechanizmu prewencyjnego dla zidentyfikowanego ryzyka, zwłaszcza zaś ryzyka o istotnym wpływie na organizację, pojawi się luka w środowisku kontroli. Wycena istotności takiej luki odbywa się najczęściej na podstawie szacunkowej wartości potencjalnej szkody, która może pojawić się w majątku przedsiębiorstwa w związku ze zmaterializowaniem się ryzyka w najczarniejszym znanym scenariuszu. Potencjalna szkoda jest przy tym wyliczana z zastosowaniem treści art. 361 § 2 KC, który stanowi, że: „naprawienie szkody obejmuje straty, które poszkodowany poniósł, oraz korzyści, które mógłby osiągnąć, gdyby mu szkody nie wyrządzono". Należy zatem wziąć pod uwagę np. maksymalną wartość kary finansowej, jaka może zostać nałożona na organizację w związku ze zdiagnozowaną luką w środowisku kontroli.

Przykład

W ramach analizy ekspozycji na ryzyko diagnozujemy, że nasza organizacja jest zobligowana do weryfikacji obecności kontrahentów na listach sankcji gospodarczych, m.in. liście osób i podmiotów objętych sankcjami dostępnej na stronie Ministerstwa Spraw Wewnętrznych i Administracji[7], listach sankcji administrowanych przez Komisję Europejską[8] oraz ONZ[9]. Brak weryfikacji obecności naszych kontrahentów na listach sankcji może prowadzić do dotkliwych kar finansowych, np. w świetle art. 149 w zw. z art. 150 ust. 3 TerroryzmU nawet do wysokości równowartości kwoty 5 000 000 euro albo do wysokości 10% obrotu wykazanego w ostatnim zatwierdzonym sprawozdaniu finansowym za rok obrotowy lub w ostatnim skonsolidowanym sprawozdaniu finansowym za rok obrotowy – w przypadku instytucji objętych skonsolidowanym sprawozdaniem finansowym grupy kapitałowej.

Wyobraźmy sobie, że ramach diagnozy środowiska kontroli ustalamy lukę w postaci braku procedury obligującej naszych pracowników do dokonywania weryfikacji obecności kontrahentów na listach sankcji, jednak nic z tym nie robimy albo przewidujemy taką procedurę, ale nie udostępniamy pracownikom adekwatnych narzędzi do jej realizacji. Podobny problem pojawi się, kiedy w ogóle nie zdiagnozujemy potrzeby weryfikacji obecności naszych kontrahentów na listach sankcji.

W sytuacji gdyby okazało się, że wśród naszych kontrahentów znajduje się podmiot objęty sankcjami, taką wiedzę uzyskamy jednak dopiero w trakcie postępowania kontrolnego ze strony organów administracji publicznej i wtedy trudno nam będzie się bronić przed potencjalną karą w sytuacji braku adekwatnego środowiska kontroli.

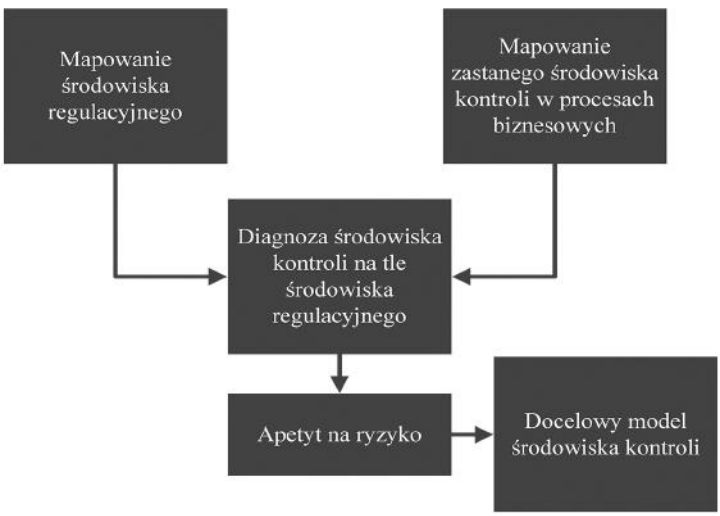
Jeżeli nie zdiagnozujemy istotnego, czyli inaczej kosztownego w przypadku kary, ryzyka regulacyjnego, a w efekcie pozostawimy je bez odpowiedzi w postaci ograniczającego ekspozycję na to ryzyko mechanizmu kontrolnego, może się okazać, że w naszym środowisku kontroli pojawi się nieświadoma luka. Lukę taką określić możemy jako niepewność środowiska kontroli, co w kontekście programu compliance jest stanem wysoce niepo-

6 Opracowanie własne oparte o badania empiryczne Autora.
7 Zob. https://www.gov.pl/web/mswia/lista-osob-i-podmiotow-objetych-sankcjami (dostęp: 25.5.2024 r.).
8 Zob. https://data.europa.eu/apps/eusanctionstracker/ (dostęp: 25.5.2024 r.).
9 Zob. https://www.un.org/securitycouncil/content/un-sc-consolidated-list (dostęp: 25.5.2024 r.).

żądanym, bo niemierzalnym. Oczywiście, niezaadresowane mechanizmem kontrolnym ryzyko może być również skutkiem świadomego **apetytu na ryzyko**, kiedy uznamy, że koszty prewencji są zbyt wysokie wobec relatywnie niskiego prawdopodobieństwa materializacji ryzyka, albo uznaniem, że nasza wycena ryzyka, czyli najczęściej ekspozycja na karę finansową, jest niższa niż koszty związane z prewencją, tj. wdrożeniem mechanizmu kontrolnego (np. przewidywane koszty technologii oraz koszty osobowe związane z zaadresowaniem zdiagnozowanego ryzyka).

W sytuacji kiedy znamy już zastane środowisko regulacyjne oraz środowisko kontroli obecne w naszej organizacji, możemy przystąpić do **oceny adekwatności środowiska kontroli odpowiadającego apetytowi na ryzyko**. Schemat procesu mapowania docelowego środowiska kontroli zaprezentowany został na rysunku 4.

Rysunek 4. Model budowy docelowego środowiska kontroli



Czynności prowadzące do ustalenia docelowego środowiska kontroli, które odpowiada naszemu apetytowi na ryzyko w otoczeniu regulacyjnym, najlepiej zaprezentować na przykładzie.

Przykład

Wyobraźmy sobie przedsiębiorcę, który prowadzi salon sprzedaży samochodów luksusowych.

W toku **mapowania zastanego środowiska regulacyjnego** ustalono, że przedsiębiorca w ramach prowadzonej działalności gospodarczej dokonuje sprzedaży samochodów w formie gotówkowej oraz bezgotówkowej. Posiada również jeden rachunek bankowy w instytucji finansowej z siedzibą w kraju UE, rachunek ten jest wykorzystywany do rozliczeń z kontrahentami oraz wpłat gotówki uzyskanej ze sprzedaży pojazdów za gotówkę. Zdarza się, że klient płaci gotówką za pojazd, którego wartość kilkakrotnie przekracza równowartość 10 000 euro.

Z powyższego stanu faktycznego wynika, że w zakresie, w jakim przedsiębiorca przyjmuje od klientów płatności w gotówce, jest instytucją obowiązaną w rozumieniu przepisów TerroryzmU. Artykuł 2 ust. 1 pkt 23 TerroryzmU wskazuje, że instytucjami obowiązanymi są m.in. przedsiębiorcy (...) w zakresie, w jakim przyjmują lub dokonują płatności za towary w gotówce o wartości równej

lub przekraczającej równowartość 10 000 euro, bez względu na to, czy transakcja jest przeprowadzana jako pojedyncza operacja, czy kilka operacji, które wydają się ze sobą powiązane.

W zakresie, w jakim przedsiębiorca przyjmuje od klientów wpłaty gotówkowe o wartości przekraczającej równowartość 10 000 euro, powinien stosować wobec klientów przewidziane w TerroryzmU środki bezpieczeństwa finansowego, a w szczególności:

1) identyfikować i weryfikować ich tożsamość, a także w uzasadnionych okolicznościach identyfikować ewentualnych beneficjentów rzeczywistych dla tych klientów, w rozumieniu art. 2 ust. 2 pkt 1 TerroryzmU;
2) oceniać ryzyko prania pieniędzy i finansowania terroryzmu po stronie klientów;
3) informować Generalnego Inspektora Informacji Finansowej o transakcjach podejrzewanych o pranie pieniędzy lub finansowanie terroryzmu, które z tym przedsiębiorcą usiłowali przeprowadzać klienci, a także o wpłatach gotówkowych klientów przewyższających równowartość 15 000 euro (w tym drugim przypadku niezależnie od podejrzenia prania pieniędzy lub finansowania terroryzmu);
4) wdrożyć procedury w zakresie przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu, a jeśli przedsiębiorca zatrudnia pracowników – także procedury raportowania podejrzenia naruszenia przepisów TerroryzmU;
5) weryfikować klientów dokonujących transakcji gotówkowych w kwotach przekraczających równowartość 10 000 euro na listach sankcji, o których mowa w art. 118 TerroryzmU.

Niezastosowanie się do powyższych obowiązków może skutkować dotkliwą odpowiedzialnością karną i administracyjną, przewidzianą w rozdziałach 13 i 14 TerroryzmU. Kary finansowe dla instytucji niefinansowych sięgają przy tym kwoty 1 000 000 euro.

W ramach mapowania zastanego środowiska kontroli ustalono także, że przedsiębiorca prowadzący salon sprzedaży samochodów luksusowych nie zdiagnozował wcześniej, że powinien stosować się do zapisów TerroryzmU, tym samym jego ekspozycja na ryzyko non-compliance (braku zgodności z regulacjami) została wyceniona na 1 mln euro, bo tyle wynosi maksymalna kara przewidziana dla tego rodzaju – tj. niefinansowej – instytucji obowiązanej.

Przedsiębiorca uznał, że tak wysoka ekspozycja na ryzyko regulacyjne przekracza jego apetyt na ryzyko, w związku z czym nie akceptuje zaistniałej luki w mechanizmach kontrolnych. Tym samym zdecydował o konieczności wdrożenia rozwiązań proceduralnych, które pozwolą na eliminację lub, co najmniej, znaczną redukcję wspomnianej ekspozycji na ryzyko, tj. o wdrożeniu docelowego modelu środowiska kontroli. W tym celu zatrudnił specjalistę ds. compliance i powierzył mu powyższe zadanie.

2.2.2. Bieżące monitorowanie zmian w środowisku ryzyka

Wdrożenie docelowego modelu środowiska kontroli oraz ewentualna zakończona sukcesem walidacja (weryfikacja) poprawności wdrożenia pozwala na przejście do kolejnego etapu cyklu zarządzania ryzykiem regulacyjnym, tj. do **bieżącego monitorowania zmian w środowisku ryzyka**.

Etap ten obejmuje w szczególności:

1) **monitorowanie zmian w regulacjach** zdiagnozowanych jako adekwatne dla naszej organizacji biznesowej;
2) **monitorowanie wytycznych regulatorów oraz organizacji branżowych** w zakresie stosowania prawa odnoszącego się o naszego przedsiębiorstwa;
3) **reakcję na zdiagnozowane incydenty naruszenia zasad compliance**, czyli przypadki, kiedy z różnych źródeł dowiadujemy się o nieprawidłowościach w funk-

cjonowaniu środowiska kontroli lub wręcz celowym pomijaniu mechanizmów kontrolnych w naszej organizacji, np. wskutek raportów sygnalistów;

4) **obserwację rynku** w kontekście trendów w stosowaniu przepisów prawa odnoszących się do naszego przedsiębiorstwa oraz wszelkich dostępnych w domenie publicznej informacji o zdiagnozowanych naruszeniach przepisów przez naszą biznesową grupę odniesienia, np. konkurencję lub członków organizacji branżowych, do których należymy.

Brak reakcji na zmianę w środowisku regulacyjnym może być przy tym postrzegany jako milcząca zgoda na nieprawidłowości, a to często prowadzi do eskalacji i multiplikacji problemów.

2.3. Przegląd orzecznictwa oraz piśmiennictwa odnoszącego się do funkcji compliance

Znaczenie programu compliance w procesie zarządzania ryzykiem regulacyjnym dostrzega już orzecznictwo sądów krajowych.

Orzecznictwo

Organizacja, która wkomponowała compliance w strukturę zarządzania budzi większe zaufanie w obrocie handlowym, ponieważ funkcje zgodności są ukierunkowane na budowanie zaufania do przedsiębiorstwa i wykrywanie ewentualnych nieprawidłowości nawet przy dobrze funkcjonującym systemie komunikacyjnym.

Działania na rzecz dochowania zgodności zmniejszają poziom ryzyka i możliwego strategicznego oportunizmu poprzez dyscyplinowanie menedżerów do odpowiednich działań. Podział kompetencji między pracowników pozwala na optymalne wykorzystanie zasobów ludzkich i kapitału, a dla zachowania wymogów przejrzystości i ochrony interesu spółki, a także samych piastunów, zasady tego podziału są dookreślane, tym bardziej że umowny podział kompetencji w stosunkach wewnątrzkorporacyjnych może powodować zaostrzenie lub złagodzenie odpowiedzialności (wyr. SN z 15.11.2022 r., II PSKP 41/22, Legalis).

Sądy w Polsce przy ocenie działania w ramach tzw. dozwolonego ryzyka gospodarczego, które nie podlega odpowiedzialności karnej, powołują się również na standard starannego działania, wskazując, że ocenie podlega stopień zabezpieczenia przedsiębiorstwa przed negatywnymi skutkami spełnienia się podjętego ryzyka (wyr. SA w Gdańsku z 23.10.2014 r., II AKa 251/14, Legalis). W kontekście wcześniejszych rozważań wzmiankowane orzeczenie sądu nawiązuje w ocenie autora do konieczności wdrożenia programu compliance obejmującego element cyklu zarządzania ryzykiem regulacyjnym.

Co więcej, w ramach weryfikacji ewentualnej odpowiedzialności karnej w orzecznictwie wskazuje się na procedurę dwuetapową:

1) po pierwsze – **należy ustalić, na podstawie abstrakcyjnego i obiektywnego modelu zachowania, granicę dopuszczalnego ryzyka w danych okolicznościach**, a dopiero wówczas
2) **odnieść do niej stopień ryzyka stwierdzonego w danej sprawie**. W praktyce może być to zadaniem dość trudnym, bowiem **organ stosujący przepisy karne**

zmuszony jest w tym zakresie dokonać czysto ekonomicznej analizy (wyr. SA w Gdańsku z 23.10.2014 r., II AKa 251/14, Legalis).

W orzecznictwie sądu wskazuje się również na „właściciela" ryzyka braku zaadresowania luki w środowisku kontroli. Osobą tą nie jest bynajmniej specjalista ds. compliance, ale zarząd lub wyższe kierownictwo.

Orzecznictwo

Podstawowym obowiązkiem zarządu jest prowadzenie spraw spółki, co polega m.in. na zarządzaniu jej majątkiem. Przy podejmowaniu decyzji dotyczących prowadzenia spraw spółki członek zarządu powinien się kierować wyłącznie jej interesem. Zawinione działania dokonane z przekroczeniem granic ryzyka gospodarczego są sprzeczne z interesem spółki i jako naruszające ogólny nakaz określony w art. 201 KSH uzasadniają odpowiedzialność członka zarządu na podstawie art. 293 § 1 KSH (wyr. SA w Poznaniu z 6.7.2017 r., I ACa 420/14, Legalis).

Nie jest zatem prawdą twierdzenie, z którym nierzadko jest konfrontowany specjalista ds. compliance, że to on odpowiada za zapewnienie skutecznego środowiska kontroli. Ostatecznie odpowiedzialność za przekroczenie granic ryzyka gospodarczego spoczywa na organie spółki lub osobie wyznaczonej przez organ do działania lub zaniechania w jej imieniu. Komórka compliance wspiera proces budowy środowiska kontroli w ramach programu compliance i monitoruje jego realizację, ale to nie compliance podejmuje decyzje gospodarcze prowadzące do odpowiedzialności karnej lub cywilnej za szkodę wyrządzoną spółce.

Orzecznictwo

Przypisanie cech przestępnych określonemu czynowi zabronionemu z art. 296 KK (bezprawności, karygodności i zawinienie w ramach działania na szkodę spółki) jest zabiegiem bardziej skomplikowanym niż w przypadku innych przestępstw z tego właśnie powodu, że wymaga uwzględnienia w karnoprawnej ocenie całej złożoności specyficznych warunków obrotu gospodarczego, a w szczególności ryzyka gospodarczego podejmowanego przez jego sprawcę. Jeżeli ryzyko to nie ma cech nadmierności, to należy wykluczyć bezprawność działań w jego ramach podejmowanych. Niegospodarność sama w sobie nie jest zjawiskiem z założenia patologicznym, bowiem stanowi nieodłączny element aktywności ekonomicznej i wynika z różnych przyczyn, począwszy od braku wiedzy i doświadczenia osoby podejmującej decyzje gospodarcze, a skończywszy na ryzyku, którym obiektywnie obarczona jest każda decyzja gospodarcza (wyr. SA w Warszawie z 10.9.2015 r., II AKa 137/15, Legalis).

W odniesieniu do sektorów regulowanych na uwagę zasługują w szczególności rekomendacje i interpretacje UKNF, który sprawuje pieczę nad podmiotami sektora usług finansowych oraz weryfikuje zgodność ich działań z przepisami prawa.

W jednym ze stanowisk UKNF można przeczytać, że: „w firmach inwestycyjnych istnieć powinny cztery podstawowe systemy wewnętrzne: kontroli wewnętrznej, zarządzania ryzykiem, audytu wewnętrznego, nadzoru zgodności działalności z prawem, tj. compliance. (...) Jakość kultury compliance ma oczywisty wpływ na poprawne funkcjonowanie innych systemów wewnętrznych, właściwe zarządzanie konfliktami interesów, poprawne przeprowadzanie transakcji własnych czy też przekłada się na poziom świadczenia usług (...). Co istotne, obszar aktywności compliance ma szeroki zasięg, gdyż

obejmuje zarówno sferę prewencji, tj. przed realizacją określonych zamierzeń, bieżącej analizy, tj. weryfikacji aktualnie podejmowanych działań firmy inwestycyjnej, jak też obszar *ex post*, tj. weryfikacji już podjętych czynności"[10].

W innym stanowisku[11] odnoszącym się do sektora ubezpieczeniowego możemy natomiast przeczytać, że: „jednym z podstawowych warunków prawidłowego wykonywania zadań przez funkcję compliance w zakładzie ubezpieczeń (...) jest posiadanie przez osobę nadzorującą tę funkcję oraz osoby wykonujące czynności należące do tej funkcji odpowiednich kompetencji, szczególnie w zakresie oceny możliwego wpływu wszelkich zmian stanu prawnego na operacje zakładu oraz określenia i oceny ryzyka związanego z nieprzestrzeganiem przepisów prawa, regulacji wewnętrznych oraz przyjętych przez zakład standardów postępowania (dalej: ryzyko braku zgodności)". Urząd Komisji Nadzoru Finansowego podkreśla zatem konieczność zapewnienia, że osoba piastująca funkcje specjalisty ds. compliance posiada dostateczną wiedzę i doświadczenie, aby móc adekwatnie monitorować zmiany w regulacjach prawnych z otoczenia branży, w której pracuje, a także ocenić ryzyko non-compliance, w przypadku zdiagnozowania luki w środowisku kontroli. Z praktycznego punktu widzenia można również oczekiwać, że w przypadku zdiagnozowania braków w kompetencjach, zidentyfikowana luka zostanie uzupełniona w postaci szkoleń lub uzyskania wsparcia zewnętrznego doradcy.

W tym samym stanowisku UKNF wskazuje, że: „Na konieczność posiadania właściwych kompetencji wskazują również takie czynniki, jak: dynamiczne zmiany otoczenia regulacyjnego, środowiska biznesowego, jak i rozwój prowadzonej działalności (np. nowe kanały dystrybucji, rozwój nowych technologii, wprowadzenie nowych przepisów prawa lub zmian w obowiązujących regulacjach prawnych).

W ocenie UKNF, w celu zapewnienia właściwego zakresu kompetencji osoby nadzorującej funkcję zgodności z przepisami oraz osób wykonujących czynności należące do tej funkcji, jak również odpowiedniej liczby osób realizujących te zadania, niezbędne jest, w pierwszej kolejności, zidentyfikowanie przez zakład zapotrzebowania na określone kompetencje dla funkcji compliance, w oparciu o obiektywne i z góry zdefiniowane kryteria, ze względu na konieczność utrzymywania przez funkcję compliance ciągłej zdolności do prawidłowego działania. W tym procesie należy uwzględniać m.in.:

1) skalę i zakres prowadzonej działalności;
2) specyfikę oferowanych produktów ubezpieczeniowych oraz kanałów dystrybucji;
3) obowiązki sprawozdawcze, a także
4) zadania i kompetencje funkcji compliance w ramach systemu kontroli wewnętrznej.

Ustalenie pożądanego zakresu kompetencji dla funkcji zgodności z przepisami, jak również odpowiedniej liczby osób realizujących zadania należące do tej funkcji, powinno

[10] Pismo KNF z 27.5.2014 r., DKR/WRM/485/60/1/2014/MK, System compliance w działalności inwestycyjnej, MoPB 2016, Nr 2, s. 2–16.

[11] Pismo UKNF z 24.6.2022 r., Stanowisko w sprawie dobrych praktyk dotyczących funkcji compliance w zakładach ubezpieczeń i zakładach reasekuracji, https://www.knf.gov.pl/knf/pl/komponenty/img/Stanowisko_dot_funkcji_zgodnosci_z_przepisami_78706.pdf (dostęp: 29.5.2024 r.).