

# Rozdział I

## Zarząd

Kwestia odpowiedzialności prawnej członków zarządu była w ciągu ostatnich lat przedmiotem sporów doktrynalnych. W nadchodzącym czasie można spodziewać się również w tym zakresie wielu zmian, w tym wejścia w życie nowych aktów prawnych, które znacznie zmienią zakres obowiązków nałożonych na członków zarządu.

Prawdopodobnie mamy przed sobą prawdziwy wysyp nowych regulacji, których źródłem będzie zarówno ustawodawca krajowy, jak i unijny. Zwłaszcza temat odpowiedzialności członków zarządu oraz przestępczości gospodarczej osób wysoko postawionych w spółkach (ang. *white collar crime*) z pewnością będzie w 2020 r. bardzo nośny.

Tematyka przestępczości tzw. białych kołnierzyków znalazła się w centrum zainteresowania polityków nie bez powodu. Wszelkie raporty poruszające tę tematykę wskazują na wielką skalę tego zjawiska i na ogromne straty ponoszone przez spółki z powodu takiej nieuczciwej działalności.

Nowa dyrektywa unijna dotycząca ochrony sygnalistów, nowelizacja ustawy o przeciwdziałaniu praniu pieniędzy i finansowaniu terroryzmu to tylko niektóre przykłady tego, że członkowie zarządu muszą bacznie obserwować swoje otoczenie prawne i być gotowi na dostosowywanie się do nadchodzących – i z Warszawy, i z Brukseli – zmian.

Zagadnienia przedstawione w niniejszym rozdziale:

- Ochrona sygnalistów i ich rola w przedsiębiorstwie
- Budowa systemów antykorupcyjnych
- Członkowie zarządu i odpowiednio umocowani menedżerowie spółek
- Reprezentowanie spółki jako pokrzywdzonego w postępowaniu karnym. Uszczelnianie systemów bezpieczeństwa korporacyjnego
- Kompetencje i reputacja w znowelizowanej ustawie o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu
- Odpowiedzialność karna kadry zarządzającej za przestępstwa lub wykroczenia przeciwko środowisku

# 1. Ochrona sygnalistów i ich rola w przedsiębiorstwie

## OPIS ZAGADNIENIA

Działalność osób zgłaszających różnego rodzaju nadużycia czy nieprawidłowości w organizacjach, czyli tzw. sygnalistów, systematycznie zyskuje na znaczeniu. Dotyczy nie tylko administracji publicznej, świata polityki czy spółek Skarbu Państwa. Konieczność identyfikowania nieprawidłowości i informowania o nich pojawia się już w odniesieniu do coraz mniejszych przedsiębiorstw.

Niezbędne staje się zatem stworzenie odpowiednich – na miarę określonej spółki – narzędzi, które osobom posiadającym informacje o nadużyciach umożliwią zgłaszanie takich zjawisk i jednocześnie zminimalizują ryzyko reperkusji i ewentualnego odwetu ze strony współpracowników, pracodawców czy innych podmiotów mających związek ze zgłaszaną sytuacją. Kluczowe przy tym staje się zapewnienie sygnalistom anonimowości.

Niewątpliwie kwestia sygnalistów jest problematyczna z perspektywy przedsiębiorców. Nie tylko wymaga ona szczególnych działań na poziomie technologicznym czy organizacyjnym, lecz także naraża członków organów spółek czy menedżerów na to, że sami staną się podmiotami, których będą dotyczyły zgłoszenia – również te nieprawdziwe. Instytucja sygnalisty wymusza więc wprowadzenie wielu rozwiązań, które zmierzać będą do zapewnienia etycznego i zgodnego z prawem prowadzenia biznesu we wszystkich obszarach działalności, tak aby możliwe było wykazanie, że:

- podmiot, organ czy inna osoba odpowiedzialna dochowali należytej staranności w zapobieżeniu nadużyciu lub naruszeniu,
- do nadużycia lub naruszenia nie doszło.

Na dzień przygotowywania niniejszego materiału jedynie kilka kategorii podmiotów jest zobowiązanych do ochrony sygnalistów. Są to:

- 1) instytucje obowiązane na podstawie ustawy z 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (j.t. Dz.U. z 2019 r. poz. 1115 ze zm.);
- 2) podmioty objęte ustawą z 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji (j.t. Dz.U. z 2019 r. poz. 1010 ze zm.) – w określonych okolicznościach;
- 3) przedsiębiorstwa z sektora rynków finansowych – na podstawie ustawy z 29 sierpnia 1997 r. – Prawo bankowe (j.t. Dz.U. z 2019 r. poz. 2357 ze zm.), rozporządzenia Ministra Rozwoju i Finansów z 6 marca 2017 r. w sprawie systemu zarządzania ryzykiem i systemu kontroli wewnętrznej, polityki wynagrodzeń oraz szczegółowego sposobu szacowania kapitału wewnętrznego w bankach (Dz.U. z 2017 r. poz. 637).

## GENEZA PROBLEMU

16 grudnia 2019 r. weszła w życie dyrektywa Parlamentu Europejskiego i Rady (UE) 2019/1937 w sprawie ochrony osób zgłaszających naruszenia prawa Unii. Jej celem jest ustanowienie wspólnych minimalnych norm zapewniających wysoki poziom ochrony osób zgłaszających naruszenia prawa UE. Dotyczy ona w szczególności następujących dziedzin:

- zamówień publicznych,

- usług, produktów i rynków finansowych oraz zapobiegania praniu pieniędzy i finansowaniu terroryzmu,
- bezpieczeństwa produktów i ich zgodności z wymogami,
- bezpieczeństwa transportu,
- ochrony środowiska,
- ochrony radiologicznej i bezpieczeństwa jądrowego,
- bezpieczeństwa żywności i pasz, zdrowia i dobrostanu zwierząt,
- zdrowia publicznego,
- ochrony konsumentów,
- ochrony prywatności i danych osobowych oraz bezpieczeństwa sieci i systemów informacyjnych,
- kwestii mających wpływ na interesy finansowe UE oraz dotyczących rynku wewnętrznego (w tym konkurencji i pomocy państwa).

Dyrektywa rozszerza zatem istotnie krąg podmiotów, które powinny wprowadzić u siebie zarówno systemy zgłaszania, jak i rozwiązania chroniące sygnalistów. Państwa członkowskie mają 2 lata na wdrożenie dyrektywy – można się zatem spodziewać, że również w Polsce zostaną w tym czasie podjęte działania na szczeblu legislacyjnym. Aktualnie prace nad projektem ustawy o ochronie sygnalistów prowadzą wspólnie Fundacja im. Stefana Batorego, Helsińska Fundacja Praw Człowieka, Forum Związków Zawodowych i Instytut Spraw Publicznych.

Niezależnie od prac nad ewentualnym projektem ustawy, należy już teraz zadbać o dobrze funkcjonujący system *compliance* w spółce, w tym identyfikację obszarów ryzyka, systemy zgłaszania i ochrony, mimo braku formalnych wymogów prawnych w tym zakresie. Zgłoszenia będą nierzadko dotyczyły zdarzeń z przeszłości.

## OCENA RYZYKA W 2020 R.

*Rysunek przedstawia skalę ryzyka: 1 – bardzo niskie; 5 – bardzo wysokie.*



## PROGNOZOWANY WZROST RYZYKA

Wzrost ryzyka przewidywany jest w organizacjach, w których nie funkcjonują systemy *compliance* oraz brak jest systematycznych audytów i szkoleń pracowników. Takie organizacje są najbardziej narażone na wypływanie, czasem również fałszywych, doniesień o nadużyciach i naruszeniach. Osoby zasiadające w organach spółek czy zajmujące kierownicze stanowiska w takich warunkach mogą mieć trudności w wykazaniu dochowania należytej staranności.

Ryzyko może zasadniczo wzrosnąć w przypadku podjęcia na nowo prac nad zmianą ustawy z 28 października 2002 r. o odpowiedzialności podmiotów zbiorowych za czyny zabronione pod groźbą kary (j.t. Dz.U. z 2020 r. poz. 358).

## BILANS OTWARCIA: CO NALEŻY ZROBIĆ, ABY SPEŁNIĆ WARUNEK DOCHOWANIA NALEŻYTEJ STARANNOŚCI

Rekomendowane działania:

- 1) identyfikacja funkcjonujących w spółce systemów i narzędzi służących przestrzeganiu zasad *compliance* (jeśli zostały wdrożone), w tym służących do zgłaszania nadużyć lub naruszeń;
- 2) przegląd procedur i polityk przedsiębiorstwa;
- 3) identyfikacja osób odpowiedzialnych za poszczególne obszary;
- 4) identyfikacja obszarów ryzyka we współpracy z osobami odpowiedzialnymi;
- 5) audyt przedsiębiorstwa lub obszarów wytypowanych na podstawie kryterium ryzyka;
- 6) wdrożenie konkluzji z audytu;
- 7) opracowanie lub aktualizacja procedur i polityk przedsiębiorstwa;
- 8) aktualizacja lub wdrożenie systemów i narzędzi służących przestrzeganiu zasad *compliance* (w tym służących do zgłaszania nadużyć lub naruszeń);
- 9) ewentualne uzyskanie certyfikatu zgodności z normą ISO 37001.

## 2. Budowa systemów antykorupcyjnych

### OPIS ZAGADNIENIA

Wewnętrzny *governance* w postaci polityk, regulaminów, kodeksów etyki i dobrych praktyk nie jest tylko stosem dokumentów przyjmowanych w milczącej postaci do wiadomości przez ich odbiorców. Skutecznie opracowane i wdrożone dokumenty wewnętrzne powinny być niejako instrukcją w danej – realnej sytuacji. Powinny odpowiadać na proste, aczkolwiek częste pytania, a także korespondować z sytuacjami w realnym życiu. Powinny zawierać wskazówki w takich kwestiach, jak kolacja z kontrahentem czy koszty upominkowych gadżetów firmowych, zaproszenia na konferencje, widowiska sportowe, jak również proces zakupowy i kontakty z dostawcami, administracją publiczną, przedstawicielami szeroko rozumianych organizacji politycznych czy zgłaszanie nietypowych sytuacji.

Prosty i jasny przekaz wynikający z dokumentacji powinien być również elementem szkoleń i edukacji. Szkolenia, którymi należy objąć wszystkie osoby pracujące w danej organizacji, powinny koncentrować się na aspektach praktycznych, dopasowanych do roli oraz funkcji w organizacji, jaką pełni dana osoba. Edukacja w procesie przeciwdziałania korupcji ma również charakter ciągły, systematyczny i powtarzalny. Warto, aby trenerzy, mający za zadanie przeprowadzenie takich szkoleń, posiadali praktyczne doświadczenia związane z efektami braku skutecznych systemów antykorupcyjnych w organizacji, dzięki czemu przekazywana przez nich wiedza daje realne wyobrażenie o powstałych konsekwencjach.

Operacyjne wdrożenie systemów antykorupcyjnych to również kwestie współpracy z partnerami, dostawcami, jednostkami zajmującymi się tą problematyką w procesach zakupowych, kontrahentami i ich weryfikacją. Często pomijanymi elementami systemu są działania