COMPLIANCE 360° W FIRMIE

Poradnik dla członków zarządu i kadr menedżerskich

kochański i partnerzy Business Law Firm

INFOR
Zał. R. Pieńkowski w 1987 r.

COMPLIANCE 360° W FIRMIE

Poradnik dla członków zarządu i kadr menedżerskich

INFOR
Zał. R. Pieńkowski w 1987 r.

Autorzy

Agnieszka Chajewska – rozdział VI
Agnieszka Choromańska-Malicka –rozdział X
Katarzyna Cybulska – rozdział VIII
Agata Dziwisz – rozdział III
Aleksander Galos – rozdział VIII
Anna Golenia – rozdział II
Anna Gwiazda – rozdział II
Marta Jaśkiewicz-Łajszczak – rozdział I
Marek Jeżewski – rozdział VII
Milena Kazanowska-Kędzierska – rozdział I
Joanna Kośmider –rozdziały VIII i IX
Amelia Krajewska – rozdział VII
Maciej Mackiewicz – rozdziały I i V
Monika Maćkowska-Morytz – rozdział V
Aleksandra Piech – rozdział V
Aleksandra Pizon-Jaworska – rozdział III
Ewa Różewicz-Czulak – rozdziały VIII i IX
Tomasz Szambelan – rozdział X
Monika Urban-Piotrowska – rozdział IV
Krzysztof Zięba – rozdział IV
Izabela Andrzejewska-Czernek – rozdział III
Natalia Basista – rozdziały II i IX

Grupa INFOR PL

Właściciel
Ryszard Pieńkowski

Prezes Zarządu
Ewa Świstuniuk

Dyrektor Centrum Wydawniczego
Marzena Nikiel

Zespół redakcyjny:
Ewa Martyna – redaktor merytoryczny
Jarosław Miller – redaktor graficzny
Agnieszka Wójcik – korekta
Kinga Pisarczyk – projekt graficzny okładki

Publikację polecają eksperci

INFOR PL S.A.
01-042 Warszawa, ul. Okopowa 58/72
www.infor.pl

Biuro Obsługi Klienta
01-042 Warszawa, ul. Okopowa 58/72
tel. 22 761 30 30, e-mail: bok@infor.pl
Infolinia: 801 626 666
Księgarnia internetowa: www.sklep.infor.pl
Profesjonalne księgarnie stacjonarne w kraju oraz księgarnie internetowe

ISBN: 978-83-8137-747-8

Spis treści

Wykaz skrótów

k.k., Kodeks karny – ustawa z 6 czerwca 1997 r. – Kodeks karny (j.t. Dz.U. z 2019 r. poz. 1950 ze zm.)

k.k.s., Kodeks karny skarbowy – ustawa z 10 września 1999 r. – Kodeks karny skarbowy (j.t. Dz.U. z 2020 r. poz. 19)

k.p.k., Kodeks postępowania karnego – ustawa z 6 czerwca 1997 r. – Kodeks postępowania karnego (j.t. Dz.U. z 2020 r. poz. 30)

k.s.h., Kodeks spółek handlowych – ustawa z 15 września 2000 r. – Kodeks spółek handlowych (j.t. Dz.U. z 2019 r. poz. 505 ze zm.)

k.w., Kodeks wykroczeń – ustawa z 20 maja 1971 r. – Kodeks wykroczeń (j.t. Dz.U. z 2019 r. poz. 821 ze zm.)

Kodeks cywilny – ustawa z 23 kwietnia 1964 r. – Kodeks cywilny (j.t. Dz.U. z 2019 r. poz. 1145 ze zm.)

k.p., Kodeks pracy – ustawa z 26 czerwca 1974 r. – Kodeks pracy (j.t. Dz.U. z 2019 r. poz. 1040 ze zm.)

nowe p.z.p., nowe Prawo zamówień publicznych – ustawa z 11 września 2019 r. – Prawo zamówień publicznych (Dz.U. z 2019 r. poz. 2019 ze zm.) – obowiązuje od 1 stycznia 2021 r.

Ordynacja podatkowa – ustawa z 29 sierpnia 1997 r. – Ordynacja podatkowa (j.t. Dz.U. z 2019 poz. 900 ze zm.)

Prawo bankowe – ustawa z 29 sierpnia 1997 r. – Prawo bankowe (j.t. Dz.U. z 2019 r. poz. 2357 ze zm.)

Prawo budowlane – ustawa z 7 lipca 1994 r. – Prawo budowlane (j.t. Dz.U. z 2019 r. poz. 1186 ze zm.)

Prawo ochrony środowiska – ustawa z 27 kwietnia 2001 r. – Prawo ochrony środowiska (j.t. Dz.U. z 2019 r. poz. 1396 ze zm.)

Prawo wodne – ustawa z 20 lipca 2017 r. – Prawo wodne (j.t. Dz.U. z 2020 r. poz. 310)

p.w.p., Prawo własności przemysłowej – ustawa z 30 czerwca 2000 r. – Prawo własności przemysłowej (j.t. Dz.U. z 2020 r. poz. 286)

p.z.p., Prawo zamówień publicznych – ustawa z 29 stycznia 2004 r. – Prawo zamówień publicznych (j.t. Dz.U. z 2019 r. poz. 1843 ze zm.) – obowiązuje do 31 grudnia 2020 r.

u.o.k.k. – ustawa z 6 lutego 2007 r. o ochronie konkurencji i konsumentów (j.t. Dz.U. z 2019 r. poz. 369 ze zm.)

ustawa o CIT – ustawa z 15 lutego 1992 r. o podatku dochodowym od osób prawnych (j.t. Dz.U. z 2019 r. poz. 865 ze zm.)

ustawa o PIT – ustawa z 26 lipca 1991 r. o podatku dochodowym od osób fizycznych (j.t. Dz.U. z 2019 r. poz. 1387 ze zm.)

ustawa o PPK – ustawa z 4 października 2018 r. o pracowniczych planach kapitałowych (Dz.U. z 2018 r. poz. 2215 ze zm.)

ustawa o VAT – ustawa z 11 marca 2004 r. o podatku od towarów i usług (j.t. Dz.U. z 2020 r. poz. 106)

Wstęp

Wobec zmian regulacyjnych, których liczba znacząco przybiera na sile szczególnie w ostatnim czasie, problematyka wdrożenia i prawidłowego stosowania przez każdego przedsiębiorcę tzw. procedur zgodności z przepisami, czyli *compliance*, jest wyjątkowo aktualna.

Rolą członka zarządu i menedżera w każdej organizacji jest realizowanie swoich obowiązków zgodnie z przepisami i pełnienie funkcji z należytą starannością. Z kolei wszelkie zaniechania są nieodłącznie powiązane z ryzykiem poniesienia osobistej odpowiedzialności (karnej lub karnoskarbowej, w tym również finansowej), a także narażenia samego przedsiębiorcy na wymierne straty finansowe. Co znamiennie, w ostatnim czasie nie tylko znacznie poszerzył się katalog obowiązków nakładanych na kadrę zarządzającą, lecz także katalog potencjalnych kar. Wzrosła również ich surowość.

Bezpieczeństwo prawne, jako fundamentalny aspekt prowadzenia biznesu, wymaga więc obecnie – jak nigdy dotąd – najwyższej uwagi i wyjątkowego zaangażowania.

Niniejsza publikacja, przygotowana przez prawników-praktyków, to nie tylko kompendium wiedzy. Stanowi ona przede wszystkim mapę drogową i zawiera wskazówki w zakresie wyzwań prawnych obecnych czasów.

Chcieliśmy zebrać w jednym miejscu kluczowe w naszej ocenie ryzyka prawne, z jakimi borykać się będą przedsiębiorcy w roku 2020 i w kolejnych latach. Zagadnienia, które omówiliśmy w publikacji, są według naszego doświadczenia najbardziej reprezentatywne w poszczególnych obszarach. Staraliśmy się w syntetycznej formie przygotować materiał będący przewodnikiem po zagrożeniach prawnych.

Pragniemy, aby nasza praca była inspiracją do wdrożenia narzędzi, mechanizmów i wewnętrznych regulacji, których celem jest zapewnienie bezpieczeństwa biznesu.

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 dotyczyć 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,

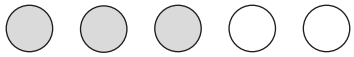
- usług, produktów i rynków finansowych oraz zapobiegania praniu pieniędzy i finansowaniu terroryzmu,
- bezpieczeństwa produktów i ich zgodności z wymogami,
- bezpieczeństwa transportu,
- ochrony środowiska,
- ochrony radiologicznej i bezpieczeństwa jądrowego,
- bezpieczeństwa żywności i pasz, zdrowia 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 odbiorów. 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

mające na celu tworzenie tzw. budżetów antykorupcyjnych, tj. takiego modelu konstruowania wynagrodzenia za pracę – w szczególności menedżerów – które niweluje ryzyko korupcji na danym stanowisku.

Wyjątkowego znaczenia nabiera również możliwość anonimowego zgłaszania sygnałów o nieprawidłowościach, zarządzania tą wiedzą w postaci wewnętrznych czynności sprawdzających i konsekwencja w egzekwowaniu wymogów wewnętrznych regulacji.

W przypadku gdy dojdzie do incydentu, kluczowego znaczenia nabiera również element dokumentowana i zbierania wszelkich możliwych informacji o nadużyciu, jakie miało miejsce w organizacji. Z punktu widzenia systemu, każde zdarzenie non *compliance* jest pouczające, a jego prawidłowa analiza prowadzi do wniosków pozwalających lepiej przeciwdziałać korupcji w organizacji.

Geneza problemu

Budowa skutecznych systemów antykorupcyjnych jest realizowana w oparciu o wiele źródeł. Mogą to być:

- wymóg prawa (np. spółki z kapitałem francuskim, brytyjskim czy amerykańskim zobowiązane są do wdrożenia systemów na podstawie odpowiednio: ustawy SAPIN 2, UK Bribery Act i US Foreign Corrupt Practices Act – FCPA);
- najlepsza praktyka oparta na standardach krajowych (wytyczne GPW w Warszawie), normach międzynarodowych (np. ISO 37001) bądź na odwołaniu do ogólnie rozumianych dobrych praktyk, które chronią spółkę czy organizację przed negatywnymi konsekwencjami korupcji.

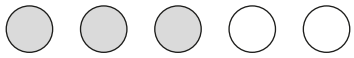
Wdrożenie skutecznych systemów antykorupcyjnych pozwala przede wszystkim zminimalizować ryzyka prawne, finansowe czy wizerunkowe grożące firmie. Dzięki wyższemu poziomowi transparentności, jaki można osiągnąć dzięki wdrożeniu systemów antykorupcyjnych, organizacja zyskuje poczucie wartości, jakie niesie za sobą dany biznes i osoby nim kierujące.

Brak wdrożenia systemów antykorupcyjnych jest również niekorzystny w kontekście badań *due dilligence*, w których taki stan może zostać oznaczony jako status „red flag". Możemy mieć również do czynienia z sytuacją najbardziej dotkliwą, w której na skutek przestępstw korupcyjnych spółka zobowiązana jest do zapłaty wielomilionowych kar. Statystycznie kary wynikające z naruszenia przepisów FCPA wynoszą rocznie 2,5 mln dolarów.

Jednym z ostatnich argumentów przemawiających za wdrożeniem systemu antykorupcyjnego w spółce jest bezpieczeństwo członków zarządu i menedżerów, którzy są prawnie zobligowani do wykazywania należytej staranności w prowadzeniu spraw spółki. Należyta staranność obejmuje wiele obszarów, w tym kwestie przeciwdziałania korupcji. Brak należytej staranności członka zarządu może być – w zależności od kontekstu – również powodem jego osobistej odpowiedzialności.

Ocena ryzyka w 2020 r.

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



Prognozowany wzrost ryzyka

Z uwagi na wiele planów legislacyjnych (np. projekty nowelizacji ustawy o odpowiedzialności podmiotów zbiorowych za czyny zagrożone pod groźną kary, projekt ustawy o jawności życia publicznego czy europejskie prawodawstwo dotyczące ochrony sygnalistów) oraz trendy światowe, przewidywać można, że problematyka związana z przeciwdziałaniem korupcji w biznesie będzie coraz bardziej aktualnym zagadnieniem w obszarze prawa.

Bilans otwarcia: co należy zrobić, aby spełnić warunek dochowania należytej staranności

Budowę systemów antykorupcyjnych możemy podzielić na kilka elementów, których dopiero całkowite wdrożenie daje możliwość uznania, że system jest skuteczny. Podkreślić należy aspekt funkcjonowania systemów antykorupcyjnych jako procesów biznesowych, a nie jednorazowych działań. Pożądanym przez spółkę stanem jest ich elastyczne współistnienie z modelem biznesowym oraz charakterystyką działalności.

Jednym z kluczowych elementów, często pomijanym przy budowaniu systemów antykorupcyjnych, jest rzetelnie przeprowadzona analiza kontekstu organizacji. W takiej analizie precyzyjnie bada się i opisuje potrzeby firmy, jej organizację, interesariuszy, otoczenie prawne i regulacyjne, podatności oraz dokonuje się oceny ryzyka.

Analiza ryzyka samej organizacji przeprowadzona – jako kolejny krok – z uwzględnieniem wyników rozważań w zakresie kontekstu organizacji powinna w efekcie dać nam wskazanie najbardziej narażonych na korupcję obszarów w firmie i przypisać im odpowiednią wagę.

Rzetelne i precyzyjne udokumentowanie podjętych działań jest pierwszym dużym krokiem w stronę budowy systemu.

Dysponując wynikami i rekomendacjami z analizy kontekstu i ryzyka, należy powołać odpowiednie funkcje w organizacji. Niezwykle istotne staje się tu nadanie pracownikom i współpracownikom kompetencji pozwalających na właściwe inspirowanie i odziaływanie na organizację. Model ten zakłada stworzenie struktury umożliwiającej prawidłowy przepływ informacji oraz pozwala na właściwe raportowanie bezpośrednio do zarządu spółki czy osób kierujących daną organizacją.

Zaangażowanie zarządu spółki jest istotne nie tylko z uwagi na aspekty świadomościowe czy wizerunkowe. Wdrożenie skutecznego systemu antykorupcyjnego wymaga nakładów i środków, nie tylko w postaci etatów, lecz także inwestycji w technologię.

Powołany *compliance officer* czy dyrektor ds. bezpieczeństwa powinni – poza kwalifikacjami merytorycznymi – być pasjonatami swojej pracy i mieć świadomość celów i oczekiwań ze strony organizacji. Role te nie są łatwe. Wielokrotnie możemy spotkać się z zarzutami hamowania biznesu i ograniczania możliwości kierowanymi pod adresem osób pełniących wzmiankowane funkcje. Bezpieczeństwo spółki i biznesu jest jednak priorytetem znacznie ważniejszym niż ryzyka, jakie mają szansę zaistnieć w sytuacji braku systemów antykorupcyjnych.

3. Członkowie zarządu i odpowiednio umocowani menedżerowie spółek

Opis zagadnienia

Dzisiejsze nadużycia i ich skala oraz ryzyka związane z przetwarzaniem ogromnych zbiorów danych, oparcie procesów biznesowych na przetwarzaniu informacji i modelach biznesowych związanych z wdrożeniami i wykorzystaniem najnowszych technologii kreują unikatowe ryzyka dla menedżerów. Największe zagrożenie dotknąć może osoby na stanowiskach kierowniczych w organizacjach, które nie wdrożyły systemów bezpieczeństwa informacji lub zrobiły to w sposób jedynie formalny.

Znikome lub mało efektywne systemy bezpieczeństwa informacji, cyberbezpieczeństwa, *compliance* czy przeciwdziałania nadużyciom w razie materializacji ryzyka i wystąpienia incydentu nie mogą przeciwdziałać negatywnym konsekwencjom prawnym. W efekcie możliwe jest wystąpienie sytuacji, w której osoba zobowiązana do dbałości o majątek reprezentowanego podmiotu i pełnienie swojej funkcji z uwzględnieniem należytej staranności może być pociągnięta do odpowiedzialności za zaniechania, jakich dopuściła się przy wdrażaniu zabezpieczeń majątku danej organizacji.

Geneza problemu

Członkowie zarządu i odpowiednio umocowani menedżerowie spółek zajmujący się sprawami majątkowymi lub działalnością gospodarczą osoby prawnej zobowiązani są do wykonywania swoich obowiązków nie tylko zgodnie z umową i przepisami prawa, lecz także z należytą starannością wynikającą z zawodowego charakteru swojej działalności. Obowiązek taki wypływa m.in. z przepisów Kodeksu spółek handlowych (art. 293 i art. 483 k.s.h.).

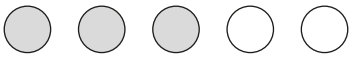
Ponadto zgodnie z art. 296 k.k., członek zarządu spółki (lub odpowiednio umocowany menedżer), który – będąc zobowiązany do zajmowania się sprawami majątkowymi lub działalnością gospodarczą osoby fizycznej, prawnej albo jednostki organizacyjnej niemającej osobowości prawnej – przez nadużycie udzielonych mu uprawnień lub niedopełnienie ciążącego na nim obowiązku wyrządza spółce znaczną szkodę majątkową, podlega odpowiedzialności karnej.

Przywołane przepisy prawa, dość dobrze znane każdemu menedżerowi, mogą nabrać nowego znaczenia w sytuacji coraz bardziej powszechnego zagrożenia cyberprzestępczością i łatwością doprowadzenia do szkody w organizacji nieprzygotowanej na nowe wyzwania bezpieczeństwa w dobie gospodarki 4.0.

Ocena ryzyka w 2020 r.

Mając na uwadze wiele norm i standardów w zakresie bezpieczeństwa, świadomość nowoczesnych *modus operandi* nadużyć i przestępstw (zwłaszcza z zakresu cyberbezpieczeństwa) oraz powinności menedżerów w dobie gospodarki 4.0, należy stwierdzić, że ryzyko powyżej określonej odpowiedzialności jest znaczne.

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



Prognozowany wzrost ryzyka

Z uwagi na rosnącą skalę nadużyć w obszarze cyberbezpieczeństwa oraz przestępstw popełnianych z wykorzystaniem nowoczesnych technologii i nieznanych dotychczas *modus operandi,* oraz fakt, że informacja i dane stanowią o sile biznesu w gospodarce 4.0, prognozuje się dalszy wzrost ryzyka w tym obszarze.

Bilans otwarcia: co należy zrobić, aby spełnić warunek dochowania należytej staranności

Rekomendowane działania:

1) zmapowanie aktywów informacyjnych w organizacji;
2) przeprowadzenie analizy ryzyka bezpieczeństwa informacji;
3) powołanie struktur odpowiedzialnych za bezpieczeństwo informacji, w tym osoby na stanowisko *Chief Security Officer;*
4) organizacja szkoleń dla pracowników;
5) przygotowanie wewnętrznego otoczenia prawnego;
6) wsparcie technologiczne;
7) przeprowadzanie cyklicznych audytów bezpieczeństwa;
8) przygotowanie organizacji do stanu dającego możliwość certyfikacji w tym zakresie normą bezpieczeństwa informacji.

4. Reprezentowanie spółki jako pokrzywdzonego w postępowaniu karnym. Uszczelnianie systemów bezpieczeństwa korporacyjnego

Opis zagadnienia

Każda spółka pokrzywdzona nadużyciem gospodarczym, rozumianym jako m.in. działania nieuczciwej konkurencji, kradzieże majątku, korupcje, podrabianie produktów, działalność nielojalnych pracowników, nadużycia podatkowe, zmowy przetargowe, cyberprzestępczość, szpiegostwo gospodarcze, może występować w postępowaniu przygotowawczym,