OCENA RYZYKA W ORGANIZACJI I ŁAŃCUCHU DOSTAW W OPARCIU O WYTYCZNE ESG

Katarzyna Saganowska, Kamila Lukowicz

ZE SZKOLENIEM ON-LINE

Wolters Kluwer

OCENA RYZYKA W ORGANIZACJI I ŁAŃCUCHU DOSTAW W OPARCIU O WYTYCZNE ESG

Katarzyna Saganowska, Kamila Lukowicz

Wolters Kluwer

WARSZAWA 2025

Stan prawny na 25 kwietnia 2025 r.

Wydawca
Jarecki Grzegorz

Redaktor prowadzący
Joanna Tchorek

Opracowanie redakcyjne
Agnieszka Witczak

Projekt okładek serii
Wojtek Janikowski, Przemek Dębowski

ISBN 978-83-8390-570-9 *ISBN PDF-a: 978-83-8390-570-9*

Wolters Kluwer Polska Sp. z o.o.
Dział Praw Autorskich
01-208 Warszawa, ul. Przyokopowa 33
tel. +48 728 313 462
e-mail: PL-ksiazki@wolterskluwer.com

księgarnia internetowa www.profinfo.pl

SPIS TREŚCI

WPROWADZENIE

Współczesne organizacje funkcjonują w dynamicznym, coraz bardziej wymagającym środowisku regulacyjnym, społecznym i rynkowym. Współczesne organizacje muszą dostrzegać wielowymiarowe korzyści wynikające z zaangażowania w działania na rzecz środowiska, społeczeństwa i ładu korporacyjnego (ESG, ang. *Environmental, Social, and Governance*). Aspekty dotyczące czynników ryzyka ESG przestały być sprowadzane jedynie do terminowego raportowania. Obecnie skuteczne zarządzanie ryzykiem w kontekście ESG wymaga holistycznego podejścia, uwzględniającego wszystkich interesariuszy, zarówno wewnętrznych, jak i zewnętrznych, regulacje oraz potencjalne zakłócenia. Tylko organizacja, która świadomie wdraża zasady ESG, buduje odporną i stabilną pozycję na rynku. Natomiast podejście ograniczone wyłącznie do spełnienia wymogów regulacyjnych niesie ryzyko niewykorzystania pełnego potencjału przy wysokich kosztach operacyjnego wdrożenia ESG w organizacji.

Przy wdrażaniu ESG kluczowe jest także uwzględnienie wpływu mediów oraz oczekiwań świadomych konsumentów, których opinie mogą mieć istotne znaczenie dla wizerunku organizacji. Brak współpracy z organizacjami pozarządowymi czy pomijanie inicjatyw społecznych może osłabić zarówno konkurencyjność, jak i reputację marki.

Istotne jest dostosowanie podejścia do specyfiki sektora i do obowiązujących regulacji, takich jak: dyrektywa NIS2, rozporządzenie DORA, RODO, dyrektywa CSRD czy niemiecka ustawa LkSG. Spójne podejście do zgodności z regulacjami oraz przypisania odpowiedzialności w organizacji konkretnym interesariuszom sprzyja optymalizacji procesów oraz

unifikacji działań. Skuteczna alokacja zasobów na budowę procesów związanych z zapewnieniem zgodności z regulacjami wymaga kompleksowego ujęcia zagadnienia. Brak scentralizowanego i holistycznego podejścia prowadzi do powielania działań, generując zbędne koszty i straty organizacyjne.

Celem niniejszej publikacji jest przedstawienie, w jaki sposób podejście holistyczne do ESG pozwala na efektywne zarządzanie ryzykiem, uniknięcie silosowego myślenia i maksymalizację wartości dla organizacji i jej interesariuszy.

Jak mawiał Winston Churchill: „Nie wystarczy, że robimy, co w naszej mocy, czasem musimy zrobić to, co jest konieczne”[1].

[1] W. Churchill, za: It Is Not Enough Quotes, https://libquotes.com/winston-churchill/quotes/it-is-not-enough

Rozdział 1

ZINTEGROWANE PODEJŚCIE DO RELACJI W BIZNESIE

1.1. Kluczowe wyzwania współczesnego zarządzania

Współczesne zarządzanie ryzykiem może być postrzegane jako wyzwanie przez wiele organizacji. Wiąże się to z kluczowymi czynnikami charakteryzującymi obecną rzeczywistość, takimi jak globalizacja, cyfryzacja, regulacje prawne oraz rosnące oczekiwania społeczne. Firmy muszą zatem dostosowywać swoje strategie do dynamicznie zmieniającego się otoczenia, w którym niepewność i złożoność stały się codziennością.

We współczesnym, dynamicznym środowisku VUCA (ang. *volatility, uncertainty, complexity, ambiguity*), które cechuje zmienność, niepewność, złożoność, niejednoznaczność, kluczowym wyzwaniem staje się zapewnienie zrównoważonego rozwoju, przy jednoczesnym zachowaniu konkurencyjności rynkowej i odporności na zagrożenia. Organizacje muszą więc działać elastycznie oraz budować strategie umożliwiające adaptację do nowych realiów (nie tylko regulacyjnych).

Coraz większą rolę w zarządzaniu i opracowywaniu strategii przedsiębiorstw odgrywają wspominane już czynniki ESG (ang. *environmental, social, governance*), które wpływają zarówno na sposób prowadzenia działalności, jak i na oczekiwania interesariuszy – od inwestorów i regulatorów, po klientów i społeczności lokalne. Firmy stają się coraz

mocniej zobowiązane do przestrzegania rygorystycznych przepisów dotyczących zrównoważonego rozwoju, raportowania niefinansowego czy zarządzania ryzykiem.

Dodatkowo postęp technologiczny oraz cyfryzacja z jednej strony otwierają nowe możliwości, ale z drugiej generują również ryzyka związane z cyberbezpieczeństwem oraz ochroną danych. Współczesne organizacje nie mogą już polegać na tradycyjnych modelach zarządzania – muszą inwestować w innowacje, rozwój kompetencji pracowników oraz budowanie odpornych łańcuchów dostaw, które pomogą im przetrwać globalne kryzysy.

W obliczu tych wyzwań niezbędne stają się partnerstwa strategiczne, współpraca międzysektorowa oraz transparentność w działaniu. W związku z tym rola interesariuszy organizacji i relacji z nimi jedynie wzrasta. Dodatkowo firmy, które potrafią skutecznie integrować odpowiedzialne zarządzanie, nowoczesne technologie oraz elastyczne modele operacyjne, nie tylko budują przewagę konkurencyjną, ale także zapewniają sobie długoterminową stabilność i wywierają pozytywny wpływ na otoczenie.

Poniżej zostaną omówione niektóre z wyzwań współczesnego zarządzania.

Transformacja cyfrowa i innowacje

Postępująca cyfryzacja, automatyzacja procesów oraz rozwój technologii wymagają od organizacji ciągłego dostosowywania swoich modeli biznesowych do nowych regulacyjnych standardów i zmieniających się realiów operacyjnych. W świecie, w którym innowacje kształtują przewagę konkurencyjną, organizacje muszą nie tylko wdrażać nowe rozwiązania technologiczne, ale również zapewniać ich bezpieczeństwo i zgodność z regulacjami. Także aby utrzymać pozycję na rynku, konkurencyjność oraz zapewnić pracownikom możliwości rozwoju, organizacje muszą uwzględniać w swojej strategii biznesowej rosnącą rolę technologii. Rozwiązania oparte na sztucznej inteligencji czy automatyzacji mogą znacząco zwiększać efektywność operacyjną, redukować koszty oraz

wspierać podejmowanie trafniejszych (ponieważ opartych na danych) decyzji. Jednak postęp technologiczny niesie również nowe zagrożenia, które wymagają wzmocnienia mechanizmów ochrony. Wzmożona potrzeba kontroli i tworzenia zabezpieczeń danych dotyczy nie tylko samej organizacji, ale również jej łańcucha dostaw, ponieważ postępująca cyfryzacja powoduje coraz to nowe zagrożenia cyberatakami. W dobie rosnącej liczby ataków hakerskich oraz zaostrzonych regulacji dotyczących ochrony danych (np. RODO[1], CCPA[2], dyrektywa NIS2[3], rozporządzenie DORA[4]), organizacje muszą inwestować w bezpieczeństwo IT, edukację pracowników oraz strategie zapobiegania cyberatakom.

Agencja Unii Europejskiej ds. Cyberbezpieczeństwa (European Union Agency for Cybersecurity, ENISA) opublikowała raport *ENISA Threat Landscape 2020*, w którym wymienia piętnaście najważniejszych cyberzagrożeń:

- złośliwe oprogramowania (*malware*),
- ataki z wykorzystaniem złośliwego kodu na stronach internetowych,
- phishing, czyli bezpośrednie lub za pomocą złośliwego oprogramowania wyłudzanie poufnych informacji,
- ataki na aplikacje internetowe,

[1] RODO – rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 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 (ogólne rozporządzenie o ochronie danych) (Dz.Urz. UE L 119, s. 1).

[2] CCPA (*California Consumer Privacy Act*) to kalifornijska ustawa o ochronie prywatności konsumentów, która weszła w życie 1.01.2020 r.

[3] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z 14.12.2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (dyrektywa NIS2), (Dz.Urz. L 333, s. 80). Dyrektywa NIS2 (*Network and Information Security Directive*). Celem tej regulacji jest wzmocnienie cyberbezpieczeństwa. Dyrektywa NIS2 zastępuje pierwotną dyrektywę NIS, wprowadza bardziej rygorystyczne wymagania dotyczące cyberbezpieczeństwa w organizacjach uznawanych za kluczowe i istotne w sektorach krytycznych.

[4] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2554 z 14.12.2022 r. w sprawie operacyjnej odporności cyfrowej sektora finansowego i zmieniające rozporządzenia (WE) nr 1060/2009, (UE) nr 648/2012, (UE) nr 600/2014, (UE) nr 909/2014 oraz (UE) 2016/1011 (Dz.Urz. UE L 333, s. 1).

- SPAM – niechciana korespondencja,
- ataki DDoS – czyli blokowanie dostępu do usług poprzez sztuczne generowanie wzmożonego ruchu,
- kradzież tożsamości,
- naruszenie poufności, integralności lub dostępności danych,
- zagrożenia wewnętrzne powodowane przez pracowników,
- botnety – sieci komputerów przejętych przez przestępców,
- ingerencja fizyczna, uszkodzenia oraz kradzież,
- wyciek danych,
- ataki ransomware w celu wyłudzenia okupu za odszyfrowanie lub nieujawnianie wykradzionych danych,
- cyberszpiegostwo,
- kradzież kryptowalut (ang. *cryptojacking*)[5].

Raport zwraca również uwagę na okoliczności, które mogą sprzyjać wzrastającej liczbie zagrożeń (obecnie warto wymienić pandemie czy konflikty zbrojne).

W związku z powyżej wymienionymi zagrożeniami organizacje powinny budować silne systemy zabezpieczeń, obejmujące nie tylko ochronę własnych danych, ale także badać bezpieczeństwo w całym łańcuchu dostaw. Organizacje są zobowiązane do wdrażania mechanizmów *compliance*, monitorowania zagrożeń oraz regularnego audytowania swoich systemów. Nie jest możliwe wyeliminowanie wszystkich potencjalnych czynników ryzyka, ale możliwe jest ograniczenie prawdopodobieństwa ich wystąpienia, wdrożenie środków prewencyjnych oraz przygotowanie scenariuszy działania po potencjalnym wystąpieniu incydentu, co buduje odpowiednią odporność na sytuacje kryzysowe.

Zmieniające się modele pracy

Pandemia COVID-19 przyspieszyła rozwój pracy zdalnej i hybrydowej. Firmy były zmuszone do zmian w przestrzeni współpracy i organizacji

[5] *ENISA Threat Landscape 2020: Cyber Attacks Becoming More Sophisticated, Targeted, Widespread and Undetected*, 20.10.2020 r., https://www.enisa.europa.eu/news/enisa-news/enisa-threat-landscape-2020 (dostęp: 16.04.2025 r.).

wewnętrznej, aby zachować ciągłość swojej działalności. Wymagało to nie tylko elastyczności w materii technologicznej, ale i tworzenia nowych modeli zarządzania. Zmiana pracy na hybrydową i zdalną spowodowała potrzebę większej kontroli w zakresie procedur dotyczących dostępu do danych, ich procesowania i animizacji.

Także dyrektywa CSRD zwraca uwagę na potrzebę budowy silnej, odpornej na zakłócenia gospodarki, nawiązując do społeczno-ekonomicznych skutków pandemii COVID-19: „Pandemia COVID-19 jeszcze bardziej przyspieszyła wzrost potrzeb użytkowników w zakresie informacji, w szczególności dlatego, że ujawniła podatność pracowników i łańcuchów wartości jednostki. Informacje na temat wpływu na środowisko są również istotne w kontekście łagodzenia przyszłych pandemii, gdyż zaburzanie ekosystemów przez człowieka jest w coraz większym stopniu powiązane z występowaniem i rozprzestrzenianiem się chorób”[6].

Pandemia COVID-19 jest również wymieniona w raporcie ENISA jako jeden z czynników, które wpłynęły na zwiększoną liczbę cyberataków. Wiązało się to z uzależnieniem zapewnienia ciągłości działania organizacji od technologii, dostępu do internetu, czyli w efekcie zwiększonego wykorzystania cyberprzestrzeni w codzienności biznesowej.

Geopolityczna destabilizacja

Świat VUCA wymaga od organizacji budowania większej odporności oraz elastyczności. Konflikty zbrojne, katastrofy naturalne, globalne kryzysy zdrowotne czy rosnące zagrożenia cybernetyczne sprawiają, że organizacje muszą dynamicznie dostosowywać swoje strategie operacyjne i rozwijać proaktywne podejście do zarządzania ryzykiem. Przerwane dostawy surowców, ograniczenia logistyczne czy wahania cen energii mogą prowadzić do poważnych problemów operacyjnych i finansowych. Szczególnie zarządzanie międzynarodowymi łańcuchami dostaw wy-

[6] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2464 z 14.12.2022 r. w sprawie zmiany rozporządzenia (UE) nr 537/2014, dyrektywy 2004/109/WE, dyrektywy 2006/43/WE oraz dyrektywy 2013/34/UE w odniesieniu do sprawozdawczości przedsiębiorstw w zakresie zrównoważonego rozwoju (Dz.Urz. UE L 322, s. 15).

maga większej dywersyfikacji i odporności na potencjalne zakłócenia oraz zapewnienia ciągłości działania. Wobec wspomnianych wyzwań wiele organizacji podążyło w kierunku nearshoringu, który ma na celu lokowanie produkcji bliżej miejsc zbytu. Organizacje redefiniują swoje podejście do zarządzania zapasami, odchodząc od modelu *just in time* (minimalizacja zapasów i uzależnienie od sprawnie działających dostaw) na rzecz *just in case* (gromadzenie strategicznych zapasów w celu zabezpieczenia się przed nagłymi zakłóceniami), mając na celu budowę bezpiecznych zapasów na wypadek podobnych zakłóceń spowodowanych czynnikami zewnętrznymi. Tworzenie bezpiecznych rezerw kluczowych komponentów i surowców staje się strategicznym elementem zarządzania ryzykiem operacyjnym, co pozwala organizacjom minimalizować skutki niespodziewanych przerw w łańcuchu dostaw.

W raporcie firmy SAP pt. *10 ryzyk związanych z łańcuchem dostaw i sposoby ich ograniczania* podkreślono, że globalne niepokoje polityczne, zmiany klimatyczne i cybernetyczne mają znaczący wpływ na stabilność łańcuchów dostaw. Organizacje ze względu na globalizację i glokalizację nie są w stanie funkcjonować bez sieci dostawców, dlatego zapewnienie ciągłości działania (ang. *Business Continuity Planning – BCP*) dla krytycznych dostaw/produktów/serwisów powinno być postrzegane w organizacji jako absolutna konieczność.

W trakcie pożarów w Australii w latach 2019 i 2020 zginęło 3 mld zwierząt, w tym zwierząt hodowlanych. Przyczyniło się to do problemów w zakresie eksportu wołowiny oraz wełny, której Australia jest głównym eksporterem do Azji. Pożary wywołały następujące skutki:

- zakłócenia w logistyce utrudniły przewóz towarów ze względu na zniszczenia dróg i infrastruktury, co również przekładało się na opóźnienia w dostawach, w szczególności w eksporcie produktów rolnych;
- spadek produkcji żywności spowodowany spłonięciem milionów hektarów terenów upraw rolnych i pastwisk;
- wpływ na produkcję węgla i rudy żelaza – surowców eksportowych;

- zniszczenie znaczących obszarów lasów wpłynęło na dostępność drewna, co z kolei doprowadziło do wzrostu cen materiałów budowlanych;
- turystyka odnotowała spadki, co miało wpływ na lokalne biznesy, restauracje i hotele.

Pożary mające miejsce w Australii są przykładem kryzysu ekologicznego, który zakłócił łańcuch dostaw na poziomie krajowym i międzynarodowym. Doskonale obrazuje, dlaczego zarządzanie ryzykiem klimatycznym oraz potrzeba dywersyfikacji powinny być włączone w długoterminowe strategie przedsiębiorców.

Rosnąca liczba wyzwań legislacyjnych

Rosnące wymagania regulacyjne w obszarach środowiskowym, społecznym i zarządczym (ang. *Environmental, Social and Governance*, *ESG*) zmuszają organizacje do dostosowania swojej działalności do coraz bardziej rygorystycznych standardów odpowiedzialnego i zrównoważonego biznesu. Przejrzystość operacyjna, etyka korporacyjna oraz wpływ na środowisko i społeczeństwo stają się najważniejszymi aspektami oceny przedsiębiorstw przez inwestorów, regulatorów oraz klientów.

Wiele organizacji już wdrożyło odpowiednie wytyczne, tworząc struktury zgodności i dostosowując je do istniejących kodeksów dobrych praktyk, takich jak:

- Kodeks Dobrych Praktyk spółek notowanych na Giełdzie Papierów Wartościowych,
- Międzynarodowe standardy ISO,
- Zasady zrównoważonego rozwoju Unii Europejskiej (*EU Principles*),
- *OECD Guidelines for Multinational Enterprises*,
- *Global Reporting Initiative* (GRI),
- czy *Sustainability Accounting Standards Board* (SASB).

Jednak integracja do modeli zarządczych odpowiedzialności za dostawców oraz całe łańcuchy wartości staje się dla wielu firm nowym, złożonym wyzwaniem. Coraz częściej organizacje muszą nie tylko ra-

portować swoje wewnętrzne działania w zakresie ESG, ale wymagać przestrzegania standardów od swoich kontrahentów czy podwykonawców oraz monitorować i oceniać (np. poprzez audyty) ich faktyczne stosowanie. Obejmuje to między innymi przestrzeganie praw człowieka, bezpiecznych warunków pracy, odpowiedzialności środowiskowej oraz zasad etyki biznesowej w całym ekosystemie dostaw.

Wraz z rosnącą liczbą regulacji organizacje muszą dostosować się do kluczowych przepisów i inicjatyw prawnych, których zakres zależy od branży, lokalizacji oraz rodzaju działalności. Poniżej kilka ważnych aktów normatywnych, które organizacje powinny uwzględnić:

- dyrektywa CSRD (*Corporate Sustainability Reporting Directive*) – wprowadza obowiązek raportowania niefinansowego dla coraz większej liczby firm, wymagając szczegółowego ujawniania informacji związanych ze wskaźnikami ESG. Zastąpiła dyrektywę NFRD (*Non-Financial Reporting Directive*), wprowadzając bardziej szczegółowe wymogi dotyczące ujawniania informacji dotyczących zagadnień środowiskowych, społecznych oraz wewnętrznego ładu korporacyjnego. Poszerza ona również krąg podmiotów zobowiązanych do raportowania oraz nakłada obowiązek audytu dla deklarowanych (raportowanych) wyników. Zadaniem organizacji jest między innymi identyfikacja negatywnego wpływu swojej działalności na środowisko oraz interesariuszy, wdrażanie działań zapobiegawczych oraz planów remediacyjnych, monitorowanie progresu realizacji założonych celów;
- Taksonomia Unii Europejskiej[7] – określa, jakie działania można uznać za zrównoważone środowiskowo, co wpływa na dostęp do finansowania i preferencyjnych warunków inwestycyjnych. Taksonomia jest powiązana z ESG, w szczególności w zakresie środowiska (*Environmental*). Pomaga na przykład zdefiniować, które działania są rzeczywiście zrównoważone środowiskowo, uwzględniając takie czynniki, jak emisje CO_2, zużycie wody, gospodarka odpadami oraz ochrona ekosystemów;

[7] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2020/852 z 18.06.2020 r. w sprawie ustanowienia ram ułatwiających zrównoważone inwestycje, zmieniające rozporządzenie (UE) 2019/2088 (Dz.Urz. UE L 198, s. 13).

- dyrektywa CSDDD[8] (*Corporate Sustainability Due Diligence Directive*) – nakłada na przedsiębiorstwa obowiązek oceny i minimalizowania negatywnego wpływu ich działalności na prawa człowieka i środowisko w całym łańcuchu wartości. Dyrektywa nie określa jednej listy wskaźników, ale organizacje będą musiały raportować zgodnie z Europejskimi Standardami Sprawozdawczości Zrównoważonego Rozwoju (ESRS). Dyrektywa CSDDD nakłada na organizacje podejmowanie działań naprawczych w przypadku zidentyfikowania negatywnego wpływu swojej działalności na środowisko lub prawa człowieka;
- regulacja SFDR (*Sustainable Finance Disclosure Regulation*) – wymaga od instytucji finansowych ujawniania informacji o wpływie ich produktów inwestycyjnych na zrównoważony rozwój;
- niemiecka ustawa o łańcuchu dostaw (*Lieferkettensorgfaltspflichtengesetz* – LkSG) – zobowiązuje duże przedsiębiorstwa do monitorowania przestrzegania praw człowieka i standardów środowiskowych przez ich dostawców;
- ustawa antykorupcyjna (UK Bribery Act, FCPA w USA) – określa zasady walki z korupcją w relacjach biznesowych, obejmując także relacje z dostawcami i partnerami handlowymi;
- dyrektywa NIS2 – zaostrza wymogi dotyczące cyberbezpieczeństwa dla kluczowych sektorów gospodarki, w tym wymaga oceny ryzyka związanego z łańcuchem dostaw;
- rozporządzenie DORA (*Digital Operational Resilience Act*) – skierowane do instytucji finansowych, wymaga od nich monitorowania ryzyk związanych z dostawcami technologii. Regulacja skupia się na odporności operacyjnej instytucji finansowych, kładąc szczególny nacisk na zarządzanie ryzykiem technologicznym i outsourcingiem IT. Wprowadza jednolite zasady dla firm finansowych i ich dostawców.

[8] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2024/1760 z 13.06.2024 r. w sprawie należytej staranności przedsiębiorstw w zakresie zrównoważonego rozwoju oraz zmieniająca dyrektywę (UE) 2019/1937 i rozporządzenie (UE) 2023/2859 (Dz.Urz. UE L 2024/1760).

Wymienione regulacje to tylko niektóre z przepisów kształtujących sposób, w jaki organizacje zarządzają ryzykiem ESG i odpowiedzialnością w ramach swoich łańcuchów dostaw. Pomimo różnych kontekstów powstania i zakresu branżowego wspomnianych aktów prawnych mają one podobny zakres wymagań dotyczących wdrożenia skutecznych mechanizmów zapewnienia należytej staranności w ocenie ryzyka (ang. *due diligence*), systemów monitorowania i audytowania partnerów biznesowych, a także zwiększonej transparentności w zakresie raportowania wpływu działalności na otoczenie.

Przedsiębiorstwa, które proaktywnie wdrażają strategie zgodności, nie tylko spełniają wymogi prawne, budują większe zaufanie na rynku, ale także zwiększają swoją odporność na ryzyka operacyjne oraz podnoszą swoją atrakcyjność w oczach inwestorów i klientów.

Rysunek 1. Przykładowe regulacje wpływające na obszary ESG

Źródło: opracowanie własne.

Nacisk ze strony interesariuszy

Współczesne organizacje funkcjonują w świecie, w którym ich działania są nieustannie oceniane przez liczne grono interesariuszy – klientów, inwestorów, pracowników oraz społeczeństwo. Wzrost świadomości społecznej, rozwój technologii oraz dostęp do informacji sprawiają, że firmy są coraz bardziej rozliczane z poziomu wiarygodności i etyki pro-

wadzenia biznesu, przestrzegania praw człowieka, wpływu na środowisko oraz sposobu zarządzania opartego na zgodności (ang. *compliance*).

Dziś bardziej niż kiedykolwiek transparentność w działalności operacyjnej, raportowaniu niefinansowym oraz realne działania oparte na wartościach deklarowanych przez organizację stają się głównymi czynnikami budowania zaufania i trwałej wartości przedsiębiorstwa. Historia pokazuje, że brak etycznego podejścia może prowadzić do spektakularnych upadków firm, które przez lata uchodziły za symbole sukcesu. Przypadki, które trwale zapisały się na kartach niechlubnej historii, takie jak Enron, WorldCom czy Carillion, unaoczniły skalę zagrożeń związanych z nieuczciwymi praktykami, manipulacjami księgowymi oraz niewłaściwym zarządzaniem. W efekcie doprowadziło to do zaostrzenia lub powstania regulacji dotyczących przejrzystości finansowej oraz odpowiedzialności zarządu, takich jak amerykańska ustawa *Sarbanes-Oxley Act* (SOX); a najnowsze regulacje unijne, na przykład dyrektywa CSRD (*Corporate Sustainability Reporting Directive*), stanowią potwierdzenie, iż regulacyjny trend się rozwija i jest utrzymywany.

W erze cyfryzacji media społecznościowe stały się potężnym narzędziem wpływu, które może zarówno wzmocnić świetną reputację firmy, jak i doprowadzić do dotkliwego i kosztownego kryzysu jej wizerunku. Społeczeństwo ma dziś więcej możliwości wyrażania swojego zdania i szybkiego mobilizowania opinii publicznej w przypadku działań firm niezgodnych z normami społecznymi czy etycznymi. Konsumenci i aktywiści z łatwością nagłaśniają skandale dotyczące nieuczciwych praktyk biznesowych, takich jak:

- zatrudnianie dzieci w łańcuchu dostaw – na przykład bojkot globalnych marek oskarżanych o wykorzystywanie nieletnich w krajach rozwijających się;
- degradacja środowiska naturalnego – szybka reakcja opinii publicznej na wycieki ropy, zanieczyszczenie oceanów plastikiem czy masowe wylesianie;
- brak odpowiedzialności społecznej – negatywny odbiór działań firm, które ignorują potrzeby swoich pracowników, złe warunki pracy w magazynach czy nierówność płac.