

COMPLIANCE W FIRMIE
– poradnik dla małych i średnich
przedsiębiorców

COMPLIANCE W FIRMIE
– poradnik dla małych i średnich
przedsiębiorców

Warszawa 2019

Compliance w firmie – poradnik dla małych i średnich przedsiębiorców

Autorzy:

Wojciech Paryś – rozdział 1

Łukasz Napiórkowski – rozdział 2

Joanna Jurasz – rozdział 3

Barbara Kaczała – rozdział 4

Klaudia Kamińska-Kiempa – rozdział 5

Redakcja: Paweł Sikorski, Filip Kolmus

Niniejsza publikacja została współfinansowana przez Komisję Europejską ze środków pochodzących z programu COSME na lata 2014–2020 oraz ze środków Ministerstwa Rozwoju w ramach programu pn. „Udział Polski w programie na rzecz konkurencyjności przedsiębiorstw oraz małych i średnich przedsiębiorstw (COSME) oraz w instrumentach finansowych programów UE wspierających konkurencyjność przedsiębiorstw w latach 2015–2021”.

Komisja Europejska, Ministerstwo Rozwoju, Polska Agencja Rozwoju Przedsiębiorczości lub osoby występujące w ich imieniu nie są odpowiedzialne za informacje przedstawione w publikacji. Poglądy wyrażone w publikacji są poglądami Autorów i nie muszą pokrywać się z działaniami Komisji Europejskiej, Ministerstwa Rozwoju oraz Polskiej Agencji Rozwoju Przedsiębiorczości.

© Copyright by Polska Agencja Rozwoju Przedsiębiorczości, Warszawa 2019

ISBN: 978-83-7633-423-3

Wydawca:

Polska Agencja Rozwoju Przedsiębiorczości ul. Pańska 81/83

00-834 Warszawa

www.parp.gov.pl

Wydanie I

Skład, łamanie i korekta:

Pracownia C&C sp. z o.o. www.ccpog.com.pl

Spis treści

Rozdział 1. Compliance – pojęcie, obszary, funkcje, wzrost znaczenia	7
1. Pojęcie „compliance”	7
1.1. Compliance jako zgodność	7
1.2. Compliance jako sposób organizacji przedsiębiorstwa	9
1.3. ISO 19600 – Compliance Management System Guidelines	10
2. Obszary compliance	11
2.1. Odpowiedzialność związana z prawem spółek.....	11
2.2. Odpowiedzialność związana z prawidłowym prowadzeniem ksiąg i rachunkowością. Odpowiedzialność karnoskarbowa	12
2.3. Odpowiedzialność związana z prawem pracy	12
2.4. Odpowiedzialność związana z korupcją	13
2.5. Ochrona danych osobowych	13
2.6. Czyny nieuczciwej konkurencji	14
2.7. Transakcje z konsumentami	14
2.8. Anti Money Laundering (AML) – przeciwdziałanie praniu brudnych pieniędzy	14
2.9. MDR – raportowanie schematów podatkowych.....	15
2.10. Prawo ochrony środowiska	16
2.11. Przepisy podatkowe	16
2.12. Zagraniczne przepisy antykorupcyjne	16
2.13. Regulacje pozaprawne	17
2.14. Podsumowanie.....	18
3. Funkcje compliance	19
3.1. Funkcja ochronna.....	19
3.2. Funkcja doradcza i informacyjna.....	20
3.3. Funkcja kontrolna i dowodowa	20
3.3.1. Funkcja gwarantowania jakości	21
4. Wzrost znaczenia	21

4.1. Początki	21
4.2. Liczba regulacji prawnych i zmienność prawa	22
4.3. Kontrole i wzrost ich skuteczności; ryzyko dla kadry Zarządzającej	24
4.4. Wzrost znajomości prawa	27
4.5. Wymóg prawny – tendencje ustawodawcze	27
4.6. Globalizacja i ujawniane afery	28
5. Compliance – aktualny stan. Raport Compliance w Polsce	29

Rozdział 2. Aktualne tendencje ustawodawcze regulujące compliance

w Polsce	32
1. Założenia dyrektywy AML VI	36
2. Projekt nowej ustawy o odpowiedzialności podmiotów zbiorowych za czyny zabronione pod groźbą kary	39
2.1. Podstawowe założenia projektowanej ustawy	43
2.2. Rozszerzenie katalogu podmiotowego ustawy poprzez zastosowanie ustawy do zagranicznych podmiotów zbiorowych	44
2.3. Czym jest czyn zabroniony w świetle nowej ustawy?	44
2.4. Jaka odpowiedzialność za czyn zabroniony?	45
2.5. Katalog kary i środków orzekanych wobec podmiotów zbiorowych	48
2.6. Zalecenia dla przedsiębiorców	49

Rozdział 3. Ochrona sygnalistów jako element efektywnej polityki

compliance	52
1. Kim jest sygnalista i jaka jest jego rola w ujawnianiu nieprawidłowości w organizacji	52
2. Ochrona sygnalistów wprowadzona na mocy Dyrektywy Parlamentu Europejskiego i Rady w sprawie ochrony osób zgłaszających przypadki naruszenia prawa Unii	57
2.1. Status quo ochrony sygnalistów w UE	57

5	<ul style="list-style-type: none"> 2.2. Skutki dla przedsiębiorców 58 2.3. Zakazane działania odwetowe 61 2.4. Przestanki objęcia sygnalisty ochroną 62 2.5. Najważniejsze środki ochrony prawnej sygnalistów 64 3. Sygnalista na gruncie prawa polskiego 64 <ul style="list-style-type: none"> 3.1. Whistleblowing w ustawie AML 65 3.2. Projekt ustawy o jawności życia publicznego 66 3.3. Projekt ustawy o odpowiedzialności podmiotów zbiorowych za czyny zabronione pod groźbą kary 67 4. Ochrona sygnalistów w Polsce – de lege ferenda 71 	58
		61
		62
		64
		64
		65
		66
		67
		71
	Rozdział 4. Rola kadry menadżerskiej 73	73
	<ul style="list-style-type: none"> 1. Etyka i zgodność z prawem w przedsiębiorstwie – motywacja do „gry fair play” 73 2. Rola kadry zarządzającej – odpowiedzialność i mechanizmy jej ograniczenia 77 <ul style="list-style-type: none"> 2.1. Definicja kadry zarządzającej 77 2.2. Odpowiedzialność członków zarządu 79 2.3. Kadra zarządzająca na straży wartości etycznych 86 3. Funkcjonowanie systemu compliance w przedsiębiorstwie: analiza ryzyka, wdrożenie, weryfikacja. Funkcja compliance oficera 88 <ul style="list-style-type: none"> 3.1. Budowa kultury organizacji 89 3.2. Sprawdzenie istniejących rozwiązań 90 3.3. Analiza ryzyka 91 3.4. Przygotowanie dedykowanych narzędzi i procedur. Funkcja compliance oficera 94 3.5. Wdrożenie i co dalej? 100 	73
		77
		77
		79
		86
		88
		89
		90
		91
		94
		100
	Rozdział 5. Compliance w prawie pracy 103	103
	<ul style="list-style-type: none"> 1. Compliance w procesie rekrutacji 104 <ul style="list-style-type: none"> 1.1. Zgodność w zakresie ochrony danych osobowych 107 	104
		107

2. Polityka antymobbingowa, niedyskryminacji i równego traktowani	111
3. Compliance w aktach wewnętrznie obowiązujących.....	121
4. Polityka zarządzania bezpieczeństwem i higieną pracy	124
5. Podsumowanie	130
O Autorach	132
O Enterprise Europe Network	134

Rozdział 1. Compliance – pojęcie, obszary, funkcje, wzrost znaczenia

Wojciech Paryś

1. Pojęcie „compliance”

W toku prowadzenia działalności gospodarczej coraz częściej można się spotkać z pojęciem compliance. Dotyczy ono nie tylko największych graczy. Również małe i średnie przedsiębiorstwa (MŚP), a nawet osoby fizyczne prowadzące jednoosobową działalność gospodarczą, mierzą się z wymogami, które niesie ze sobą compliance.

W związku z tym coraz ważniejsze jest udzielenie odpowiedzi na pytanie, czym jest compliance i jakie ma ono znaczenie dla prowadzenia działalności gospodarczej.

1.1. Compliance jako zgodność

Pojęcie compliance pochodzi od angielskiego czasownika „to comply”, czyli stosować się do czegoś. Rzeczownik „compliance” oznacza zaś „zgodność”¹.

¹ Słownik internetowy PONS: <https://pl.pons.com/t%C5%82umaczenie?q=compliance&l=en&in=&lf=en&qnac=> (data dostępu: 2 września 2019 r.).

Choć w fachowej literaturze wskazuje się², że sformułowanie prawidłowej definicji compliance jest zadaniem trudnym, to wydaje się, że słownikowe tłumaczenie tego pojęcia dobrze oddaje intuicje dotyczące znaczenia compliance. Jest tak, ponieważ – mówiąc najogólniej – compliance to właśnie zgodność z pewnymi normami, do których przestrzegania dany podmiot jest zobowiązany.

Rozbieżności w rozumieniu pojęcia compliance wynikają z różnego wyznaczania zakresu tego pojęcia. Część autorów twierdzi bowiem, że compliance to zgodność wyłącznie z powszechnie obowiązującymi normami prawnymi. Inni ograniczają znaczenie compliance wyłącznie do tych przepisów prawnych, których naruszenie może się wiązać z odpowiedzialnością karną³. Wydaje się jednak, że większość autorów, jak również dominująca część biznesu rozumie to pojęcie szeroko, tj. jako zgodność zarówno z powszechnie obowiązującymi przepisami prawnymi – w tym również tymi, które nie mają charakteru karnego – jak i ze standardami pozaprawnymi, do przestrzegania których dany podmiot sam się zobowiązał.

Przyjęcie danego rozumienia pojęcia compliance ma daleko idące konsekwencje praktyczne, bowiem to właśnie ono będzie wyznaczało zakres zobowiązania przedsiębiorstwa, a precyzując – jego władz, czyli zarządu, rady nadzorczej itd., do zapewnienia zgodności. W przypadku przyjęcia szerokiej definicji compliance przedsiębiorstwo, które zamierza wprowadzać procedury compliance, będzie musiało zapewnić zgodność również z normami pozaprawnymi, tj. przykładowo wszelkimi regułami postępowania, kodeksami etycznymi, normami jakości, zasadami

² Np. B. Jurta, Wolters Kluwer, w *Rola Organów Spółki Kapitałowej w realizacji funkcji compliance*, Warszawa 2017.

³ Np. K. Moosmayer, *Compliance. Praxisleitfaden für Unternehmen*, Monachium 2012.

dotyczącymi tzw. społecznej odpowiedzialności biznesu (ang. *corporate social responsibility* – CSR), misją przedsiębiorstwa itd.

Powyższe szerokie rozumienie compliance zdaje się być najbardziej rozpowszechnione i właśnie takie rozumienie przyjęto na potrzeby niniejszej publikacji.

1.2. Compliance jako sposób organizacji przedsiębiorstwa

W zależności od kontekstu compliance może oznaczać również pewien sposób organizacji przedsiębiorstwa oraz zespół środków zmierzających do zapewnienia zgodności z przepisami prawa oraz normami o charakterze poprawnym. Takie rozumienie compliance jest utożsamiane zatem z tzw. systemem zarządzania compliance (ang. *compliance management system* – CMS).

Podkreślenia wymaga fakt, że celem systemu zarządzania compliance jest w pierwszej kolejności prewencja. CMS winien być zatem konstruowany w taki sposób, aby nie tylko wykrywał nieprawidłowości w funkcjonowaniu przedsiębiorstwa, lecz również by im zapobiegał. Z kolei w przypadku zaistnienia danej nieprawidłowości, CMS winien pozwalać na jej szybkie wykrycie oraz na jednoznaczne ustalenie osoby odpowiedzialnej. Elementem CMS jest również takie jego ciągłe doskonalenie, by w przyszłości nie dochodziło do naruszeń.

Jak zostało wskazane, na CMS składa się pewien zespół środków. Jakich? To zależy przede wszystkim od przedmiotu działalności danego przedsiębiorstwa. Istnieje jednak pewna grupa środków, które winny być stosowane w większości przedsiębiorstw, bowiem dotyczą one wszystkich uczestników rynku. Wśród takich środków można wymienić wprowadzanie

niektórych procedur, np. procedury antykorupcyjnej (polityka przyjmowania prezentów, polityka sponsoringu) czy anonimowego zgłaszania naruszeń (tzw. sygnalistów, ang. *whistleblowing*).

Przy omawianiu pojęcia compliance warto podkreślić, że CMS to system środków, które powinny być **faktycznie stosowane** w toku prowadzenia działalności gospodarczej. Nie jest to zatem wyłącznie zestaw zasad, które po spisaniu nie mają żadnego przełożenia na praktyczne działania. Procedury winny stanowić pewien wzorzec postępowania, a pracownicy oraz w niektórych sytuacjach również kontrahenci, winni się do nich stosować na bieżąco.

Powyższe prowadzi do wniosku, że prawidłowy system zarządzania compliance gwarantuje również, że wszyscy zainteresowani, tzn. pracownicy, współpracownicy, kontrahenci, kadra kierownicza itd., powinni w niezbędnym zakresie znać odpowiednie procedury i umieć je stosować w praktyce.

1.3. ISO 19600 – Compliance Management System – Guidelines

Zainteresowanie tematyką compliance zaowocowało wydaniem w 2014 r. normy ISO 19600 dotyczącej systemu zarządzania compliance⁴. Posługuje się ona pojęciem compliance jako zgodnością, tj. spełnieniem wszystkich wymogów.

W tym miejscu warto zauważyć, że norma ISO 19600 ma charakter ogólny, który pozwala korzystać z niej przy konstruowaniu systemów zarządzania compliance w różnych przedsiębiorstwach niezależnie od ich wielkości i przedmiotu działania.

⁴ Norma nie jest aktualnie przetłumaczona na język polski.

2. Obszary compliance

To, jakie obszary powinny zostać objęte systemem zarządzania compliance, zależy przede wszystkim od przedmiotu działalności przedsiębiorcy i co się z tym wiąże – od ryzyk, jakie pojawiają się przy prowadzeniu działalności danego rodzaju. Dla przykładu można wymienić poniższe obszary.

2.1. Odpowiedzialność związana z prawem spółek

Kodeks spółek handlowych⁵ przewiduje szereg norm, których nieprzestrzeganie może się wiązać z odpowiedzialnością karną. Wśród nich można wymienić przykładowo odpowiedzialność karną zarządu za niezłożenie listy wspólników do sądu rejestrowego lub nieprowadzenie księgi udziałów czy też niezwoływanie zgromadzenia wspólników (art. 544 ksh). Z odpowiedzialnością karną może się wiązać również ogłoszenie nieprawdziwych danych, o których mowa w tytułach III i IV ksh lub też przedłożenie nieprawdziwych danych organom spółki lub władzom państwowym (art. 587 ksh). Może tu chodzić przykładowo o niezgłoszenie zwrotu dopłat w spółce z ograniczoną odpowiedzialnością lub brak dokonania ogłoszenia zawierającego wezwanie wierzycieli w toku likwidacji spółki.

Przykładem jest również odpowiedzialność karna związana z brakiem złożenia wniosku o ogłoszenie upadłości (art. 586 ksh). Warto zwrócić uwagę, że brak złożenia takiego wniosku lub jego spóźnione złożenie może wiązać się również z odpowiedzialnością odszkodowawczą zarządu (art. 299 ksh).

⁵ Ustawa z dnia 15 września 2000 r. Kodeks spółek handlowych (t.j. Dz.U. z 2019 r. poz. 505 z późn. zm.); ksh.

2.2. Odpowiedzialność związana z prawidłowym prowadzeniem ksiąg i rachunkowością.

Odpowiedzialność karnoskarbowa

Szereg przestępstw lub wykroczeń przewiduje ustawa o rachunkowości⁶. Część z tych czynów jest penalizowanych również w kodeksie karnoskarbowym⁷, który wprowadza kolejne kategorie przestępstw. Na przykład czynem karalnym jest nieprowadzenie ksiąg rachunkowych lub podawanie w nich nierzetelnych danych (art. 77 ustawy o rachunkowości oraz art. 61 kks), jak również nieskładanie sprawozdania finansowego do ogłoszenia (art. 79 ustawy o rachunkowości).

Warto zwrócić uwagę, że zgodnie z kodeksem karnoskarbowym za przestępstwa skarbowe lub wykroczenia skarbowe odpowiada, jak sprawca, także ten, kto na podstawie przepisu prawa, decyzji właściwego organu, umowy lub faktycznego wykonywania zajmuje się sprawami gospodarczymi, w szczególności finansowymi, osoby fizycznej, osoby prawnej albo jednostki organizacyjnej niemającej osobowości prawnej.

2.3. Odpowiedzialność związana z prawem pracy

Również kodeks pracy⁸ przewiduje odpowiedzialność za naruszenia. Przykładowo można wskazać na zawieranie umów cywilnoprawnych w warunkach, w których zgodnie z przepisami powinna zostać zawarta umowa o pracę (art. 281 kp) – dopuszczanie się takiego procederu może się wiązać z odpowiedzialnością administracyjną, cywilną i karną.

⁶ Ustawa z dnia 29 września 1994 r. o rachunkowości (t.j. Dz.U. z 2019 r. poz. 351).

⁷ Ustawa z dnia 10 września 1999 r. Kodeks karny skarbowy (t.j. Dz.U. z 2018 r. poz. 1958 z późn. zm.); kks.

⁸ Ustawa z dnia 26 czerwca 1974 r. Kodeks pracy (t.j. Dz.U. z 2019 r. poz. 1040 z późn. zm.); kp.

Kolejnym przykładem może być niedopełnianie obowiązku zapewnienia terminowości wypłat wynagrodzeń lub przeciwdziałania mobbingowi. Jeżeli takie zachowania mają charakter złośliwy lub uporczywy, to mogą wiązać się z ryzykiem orzeczenia nawet kary pozbawienia wolności do lat dwóch. Przykładem nowych obowiązków dla pracodawców jest obowiązek zawarcia umowy o zarządzanie pracowniczym planem kapitałowym⁹.

2.4. Odpowiedzialność związana z korupcją

Kodeks karny przewiduje sankcje w przypadku uzależnienia nadużycia uprawnień lub niedopełnienia obowiązku przez osobę pełniącą funkcję kierowniczą od udzielenia jej korzyści majątkowej lub osobistej (art. 296a kk).

2.5. Ochrona danych osobowych

RODO¹⁰ przewiduje szereg kar administracyjnych związanych z naruszaniem zasad przetwarzania danych osobowych, w tym również karę pieniężną w wysokości do 20 milionów euro. Jako przykład, że te przepisy faktycznie są egzekwowane, można wskazać karę wymierzoną Morele.net (ok. 2.8 mln złotych – wrzesień 2019 r.) lub karę wymierzoną Dolnośląskiemu Związkowi Piłki Nożnej (ok. 55 tys. złotych – maj 2019 r.).

⁹ Art. 106 Ustawy z dnia 4 października 2018 r. o pracowniczych planach kapitałowych (Dz.U. poz. 2215 z późn. zm.). Obowiązek ten wprowadzany jest stopniowo, w różnych terminach dla pracodawców w zależności od liczby zatrudnianych pracowników.

¹⁰ Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. U. UE L z 2016 r. Nr 119, s. 1 z późn. zm.).

2.6. Czyny nieuczciwej konkurencji

Przedsiębiorca winien również przestrzegać ustawy o zwalczaniu nieuczciwej konkurencji¹¹, która przykładowo nakłada obowiązek przestrzegania tajemnicy przedsiębiorstwa kontrahenta (np. art. 23) czy zakazuje organizowania sprzedaży premiowej (art. 17a).

2.7. Transakcje z konsumentami

Podmioty zawierające umowy z konsumentami powinny również mieć na uwadze zakaz używania tzw. klauzul abuzywnych (tj. niedozwolonych klauzul umownych). Ich stosowanie naraża przedsiębiorcę w niektórych przypadkach na karę administracyjną w wysokości do 10% obrotu osiągniętego w roku obrotowym poprzedzającym rok nałożenia kary (art. 106 ustawy o ochronie konkurencji i konsumentów¹²).

2.8. Anti Money Laundering (AML) – przeciwdziałanie praniu brudnych pieniędzy

Kolejnym przykładem przepisów, które nakładają na przedsiębiorców dodatkowe obowiązki, jest ustawa o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu¹³, implementująca do polskiego porządku

¹¹ Ustawa z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji (t.j. Dz.U. z 2019 r. poz. 1010).

¹² Ustawa z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów (t.j. Dz.U. z 2019 r. poz. 369 z późn. zm.).

¹³ Ustawa z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (t.j. Dz.U. z 2019 r. poz. 1115 z późn. zm.).

prawnego dyrektywę Parlamentu Europejskiego i Rady (UE) 2015/849¹⁴. Ustawa zobowiązuje tzw. instytucje obowiązane między innymi do identyfikowania oraz weryfikowania beneficjentów rzeczywistych swoich kontrahentów, jak również do wprowadzenia procedury anonimowanego dokonywania zgłoszeń naruszeń (art. 53).

2.9. MDR – raportowanie schematów podatkowych

Od 1 stycznia 2019 r. wprowadzono do polskiego porządku prawnego obowiązek raportowania tzw. schematów podatkowych (ang. *mandatory disclosure rules* – MDR). Obowiązek raportowania schematów podatkowych stanowi wynik implementacji Dyrektywy Rady (UE) 2018/822 z dnia 25 maja 2018 r.¹⁵ i znalazł odzwierciedlenie w art. 86a i nast. ordynacji podatkowej¹⁶. W myśl przepisów przedsiębiorcy oraz poszczególne osoby fizyczne działające na rzecz danego przedsiębiorcy (korzystający, promotor, wspomagający) mają obowiązek raportowania schematów podatkowych. Niedopełnienie obowiązku lub jego nieterminowe dopełnienie może się wiązać z grzywnami.

¹⁴ Dyrektywa Parlamentu Europejskiego i Rady (UE) 2015/849 z dnia 20 maja 2015 r. w sprawie zapobiegania wykorzystywaniu systemu finansowego do prania pieniędzy lub finansowania terroryzmu, zmieniająca rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 648/2012 i uchylająca dyrektywę Parlamentu Europejskiego i Rady 2005/60/WE oraz dyrektywę Komisji 2006/70/WE (Dz. U. UE L z 2015 r. Nr 141, s. 73 z późn. zm.).

¹⁵ Dyrektywa Rady (UE) 2018/822 z dnia 25 maja 2018 r. zmieniająca dyrektywę 2011/16/UE w zakresie obowiązkowej automatycznej wymiany informacji w dziedzinie opodatkowania w odniesieniu do podlegających zgłoszeniu uzgodnień transgranicznych (Dz. U. UE L z 2018 r. Nr 139, s.1 z późn. zm.).

¹⁶ Ustawa z dnia 29 sierpnia 1997 r. – Ordynacja podatkowa (t.j. Dz. U. z 2019 r. poz. 900 z późn. zm.).

2.10. Prawo ochrony środowiska

Szeroką dziedziną, w której każdy przedsiębiorca winien zapewnić zgodność, jest ochrona środowiska. Prawo ochrony środowiska to cały szereg aktów prawnych, tzn. ustaw i rozporządzeń, które przedsiębiorca powinien stosować. Naruszenia w tym zakresie, chociażby niedopełnienie obowiązków raportowania czy brak posiadania odpowiednich zezwoleń, mogą mieć poważne negatywne konsekwencje dla przedsiębiorcy.

2.11. Przepisy podatkowe

Kolejnym obszarem jest prawo podatkowe. Wobec dużej zmienności przepisów podatkowych, jak również wobec zmian interpretacyjnych istniejących przepisów, wyzwaniem z zakresu compliance jest prawidłowe zorganizowanie procesu przepływu informacji w taki sposób, by osoby odpowiedzialne były w stanie na bieżąco aktualizować swoją wiedzę w tym zakresie, jak również by zapewnić możliwość dokonywania zmian w umowach z kontrahentami, tak by nie rodziły one ryzyk podatkowych.

2.12. Zagraniczne przepisy antykorupcyjne

Aktualnie w transakcjach z podmiotami pochodzącymi spoza Polski spotyka się również postanowienia umowne, które zobowiązują kontrahentów do zgodności z prawem obcym. Nierzadko zgoda na takie zapisy stanowi warunek konieczny zawarcia umowy. Przykładem takich regulacji jest:

- Amerykański Foreign Corrupt Practices Act z 1977 r. (FCPA) – akt regulujący kwestię korupcji funkcjonariuszy publicznych;
- Brytyjski Bribery Act z 2010 r. – akt regulujący kwestię korupcji. Bribery Act wprowadza możliwość ponoszenia odpowiedzialności przez kadrę kierowniczą (ang. *senior officer*) za czyn pracownika, jeżeli czynu

korupcyjnego dopuszczono się za zgodą kierownictwa lub popełnienie tego czynu było tolerowane.

Warto zauważyć, że obowiązek przestrzegania ww. aktów prawnych często połączony jest z obowiązkiem posiadania i stosowania polityki antykorupcyjnej uwzględniającej ww. regulacje.

W tym miejscu warto również zwrócić uwagę, że wspomniane akty prawne mają bardzo szerokie zastosowanie i możliwe jest, by obowiązywały również polskiego przedsiębiorcę, który dokonuje transakcji z kontrahentem pochodzącym ze Stanów Zjednoczonych lub Wielkiej Brytanii.

2.13. Regulacje pozaprawne

Obszarem obejmowanym przez system zarządzania compliance są także regulacje pozaprawne, których przestrzeganie jest zależne wyłącznie od woli przedsiębiorcy. Obowiązek przestrzegania takich norm może wynikać również z zawartych umów cywilnoprawnych. Wśród tego typu regulacji można wymienić przykładowo:

1. międzynarodowe lub krajowe standardy i normy:

- normy ISO – w obrocie gospodarczym można spotkać się przykładowo ze zobowiązaniami dotyczącymi przestrzegania normy PN-EN ISO/IEC 27001:2017-06, która reguluje kwestie ustanowienia, wdrożenia i utrzymania systemu zarządzania informacją lub normy PN-EN ISO 9001:2015 określającej wymagania dla systemów zarządzania jakością;
- standardy wyznaczone przez OECD: G20/OECD Principles of Corporate Governance¹⁷, odnoszące się do organizacji ładu korporacyjnego;

¹⁷ https://www.oecd-ilibrary.org/governance/g20-oecd-principles-of-corporate-governance-2015_9789264236882-en (data dostępu: 2 września 2019 r.)

- kodeksy dobrych praktyk odnoszących się do danego rodzaju działalności;
2. standardy i polityki ustalane przez samego przedsiębiorcę:
- kodeks postępowania lub kodeks etyczny (ang. *code of conduct*, *code of ethics*) – można spotkać się również z innymi określeniami;
 - polityka dotycząca społecznej odpowiedzialności biznesu (polityka CSR);
 - misja przedsiębiorstwa (ang. *mission statement*), określana też czasem deklaracją programową; misja przedsiębiorstwa określa rolę danego przedsiębiorcy w kontekście jego znaczenia dla otoczenia.

Standardy i polityki stanowane przez samego przedsiębiorcę mogą przybierać różne formy. Nierzadko kodeks postępowania zawiera również deklarację programową lub politykę CSR.

2.14. Podsumowanie

Powyższe wyliczenie nie ma charakteru zupełnego. Również przykłady podane w poszczególnych obszarach nie zawsze są reprezentatywne dla danego obszaru. Celem wcześniejszego wyliczenia jest ukazanie, że system zarządzania compliance to niejako klamra organizacyjna spinająca strukturę przedsiębiorcy w taki sposób, by zapewniać zgodność działań przedsiębiorcy ze wszystkimi – często bardzo odległymi – obszarami.

Jak zostało wskazane na wstępie, zakres, do którego może odnosić się system zarządzania compliance, wynika w znacznym stopniu z przedmiotu działalności danego przedsiębiorcy i może być szerszy – np. wtedy, kiedy przedsiębiorca podlega regulacjom sektorowym, jak choćby prawu energetycznemu czy prawu medycznemu, lub też węższy – np. wtedy, kiedy dany przedsiębiorca nie jest instytucją obowiązana zgodnie z ustawą o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu. Niezależnie jednak od zakresu, do jakiego system zarządzania compliance

u danego przedsiębiorcy będzie się stosował, to zadaniem CMS będzie zapewnienie zgodności działań przedsiębiorcy, jego pracowników, współpracowników i kadry zarządzającej z normami prawnymi i pozaprawnymi, które są istotne z punktu widzenia tego przedsiębiorcy, jak również identyfikacja naruszeń, które miały miejsce oraz ciągłe doskonalenie organizacji.

3. Funkcje compliance

Compliance jako system zapewnienia zgodności pełni w przedsiębiorstwie szereg funkcji¹⁸.

3.1. Funkcja ochronna

Ochrona interesów przedsiębiorcy, jego kadry zarządzającej oraz pracowników i kontrahentów to podstawowa funkcja compliance. CMS powinien działać prewencyjnie i chronić przedsiębiorcę przed ryzykiem wystąpienia naruszeń, które mogą jego lub zatrudnionych przez niego pracowników narazić na sankcje, a przynajmniej znacząco wspomniane ryzyko obniżyć.

W przypadku wystąpienia naruszeń CMS powinien również pozwalać na ich identyfikację oraz przeprowadzenie procedury naprawczej (np. system anonimowego zgłaszania naruszeń).

Okoliczność posiadania i stosowania CMS może być również brana pod uwagę przy wymierzaniu sankcji w przypadku wystąpienia naruszeń.

¹⁸ Klasyfikacja za: B. Jaruga, *Rola organów spółki kapitałowej w realizacji funkcji compliance*, Wolters Kluwer Polska S.A., Warszawa 2017.

3.2. Funkcja doradcza i informacyjna

Prawidłowo działający system zarządzania zgodnością pełni również funkcję doradczą i informacyjną. Wprowadzone w przedsiębiorstwie procedury powinny stanowić wzorzec zachowania dla pracowników i przewidywać również sytuacje nietypowe i rzadko spotykane. Takim przykładem jest procedura odnosząca się do kontroli organów państwowych (np. prokuratura lub PIP). Oczywiście, by funkcja doradcza mogła być realizowana w pełni, stosowni pracownicy powinni mieć wiedzę o istnieniu procedury danego typu i miejscu, gdzie można ją znaleźć, o ile nie znają jej treści.

System CMS winien również na bieżąco prowadzić do aktualizacji wiedzy na temat zmieniającego się otoczenia prawnego i konsekwencji naruszeń.

3.3. Funkcja kontrolna i dowodowa

Kolejnymi funkcjami, jakie są realizowane przez CMS, są funkcje kontrolne i dowodowe. Istota funkcji kontrolnej sprowadza się do dokonywania weryfikacji stosowania procedur i sprawdzania, czy w danych sytuacjach organizacja zachowuje się w sposób zgodny z prawem i pozostałymi obowiązującymi ją normami. Zalecane jest przy tym, by tego typu kontrole przeprowadzono cyklicznie.

Z kolei funkcja dowodowa CMS to nic innego jak gromadzenie dokumentacji, stanowiącej dowód działania systemu compliance w przedsiębiorstwie. Przykładem tego typu dokumentacji mogą być protokoły z audytów wewnętrznych czy notatka służbowa z dokonania czynności. Gromadzenie dowodów może odgrywać niebagatelną rolę przy wykazywaniu, że kadra zarządzająca dochowała należytej staranności.

3.4. Funkcja gwarantowania jakości

Działający CMS eliminuje nieprawidłowości i ogranicza ryzyko naruszeń. Dzięki temu system zarządzania compliance stanowi równocześnie gwarancję jakości, wymaganej w relacjach biznesowych.

3.5. Funkcja marketingowa

Presja na rynku powoduje generowanie nowych obszarów, w których przedsiębiorcy mogą konkurować. Posiadanie CMS może stanowić walor przesądający lub stanowiący warunek konieczny zawarcia umowy z kontrahentem. CMS stanowi również jeden z elementów wpływających na reputację i zaufanie do przedsiębiorcy.

4. Wzrost znaczenia compliance

4.1. Początki

Historia compliance sięga początku XX w. Wskazuje się, że pierwsze regulacje dotyczące systemu zarządzania compliance były skutkiem powołania do życia w Stanach Zjednoczonych szeregu instytucji państwowych, których celem było zapewnienie bezpieczeństwa publicznego (np. Agencja ds. Żywności i Leków). Rozwój compliance rozpoczyna się jednak na przełomie lat 60. i 70. ubiegłego wieku, kiedy to doszło do wykrycia nadużyć dotyczących prawa ochrony konkurencji. Wdrażane systemy compliance miały zapobiec w przyszłości niezgodnemu z prawem podziałowi rynku przez firmy z branży

przemysłu elektrycznego¹⁹. Kolejnym krokiem było wykrycie szeregu afer korupcyjnych, w tym afery Watergate, i związanym z tym uchwaleniem w 1977 r. wspomianej już powyżej Foreign Corrupt Practices Act.

Wydaje się jednak, że najważniejszym momentem, który zdecydował o szybkim wzroście znaczenia compliance w przedsiębiorstwach, było ustanowienie na początku lat 90. XX wieku przez amerykańską Komisję ds. wymiaru kar (ang. *Sentencing Commission*) Federalnych Wytycznych Wymiaru Kar, zgodnie z którymi okolicznością łagodzącą jest to, iż dany przedsiębiorca stosuje środki mające na celu przeciwdziałanie wypadkom naruszenia prawa.

W ostatnich kilkunastu latach wzrost znaczenia compliance jest wyraźnie odczuwalny również w Polsce. Wydaje się, że decydujące znaczenie mają tu czynniki opisane niżej.

4.2. Liczba regulacji prawnych i zmienność prawa

Jednym z najważniejszych czynników, wpływających na wzrost znaczenia compliance i zainteresowanie praktycznym wymiarem CMS, jest znaczny przyrost przepisów prawnych połączony ze wzrostem ich skomplikowania oraz wzajemnych powiązań.

¹⁹ B. Jaruga, *Rola organów spółki kapitałowej w realizacji funkcji compliance*, Wolters Kluwer Polska S.A., Warszawa 2017.

Wzrost liczby aktów prawnych dobrze obrazują następujące dane²⁰:

<i>Liczba stron aktów prawnych, które weszły w życie w poszczególnych latach</i>											
Rok	1989	1997	2000	2001	2004	2011	2015	2016	2017	2018	2019 (prognoza)
Liczba stron	1186	5672	7016	12941	20059	16387	24781	35280	23681	20325	21524

Jak wynika z powyższych danych, od 1989 r. do rekordowego 2016 r. liczba stron aktów prawnych, które weszły w życie w danym roku, wzrosła prawie 30-krotnie (z 1186 stron do 35 280 stron). Dopiero od dwóch lat, tj. od 2017 r., widać spadek produkcji prawa w Polsce. Prognoza na rok 2019 wskazuje, że liczba stron aktów prawnych wchodzących w życie w roku 2019 przekroczy 21 tysięcy.

Znamienne są też dane dotyczące zmienności prawa²¹. W latach 2012–2014 w Polsce wyprodukowano średnio 56 razy więcej przepisów niż w Szwecji i 11 razy więcej niż na Litwie.

Przy tak wielu nowych przepisach, jak również ich zmienności, system zarządzania compliance stanowi dobre rozwiązanie pozwalające śledzić na bieżąco istotne zmiany i ograniczać w ten sposób ryzyko naruszeń.

²⁰ Dane na podstawie raportu: Barometr stabilności otoczenia prawnego w Polsce; Grant Thornton. <http://barometrprawa.pl/#barometr>

²¹ Dane na podstawie raportu: *Firmy w kagańcu regulacji; Polska liderem Unii Europejskiej w produkcji prawa*; Grant Thornton, <http://barometrprawa.pl/#wykresy>.

4.3. Kontrole i wzrost ich skuteczności; ryzyko dla kadry zarządzającej

Drugą ważną przyczyną wzrostu znaczenia compliance w Polsce jest wzrost skuteczności kontroli przeprowadzanych przez organy publiczne. Z danych przedstawionych przez Krajową Administrację Skarbową wynika, że²²:

- w 2015 r. przeprowadzono ok. 48 tys. kontroli i w ich wyniku uzyskano ok. 3097 mln zł wpływu;
- w 2016 r. przeprowadzono ok. 38 tys. kontroli i w ich wyniku uzyskano ok. 3464 mln zł wpływu;
- w 2017 r. przeprowadzono ok. 27 tys. kontroli i w ich wyniku uzyskano ok. 5061 mln zł wpływu.

Powyższe dane wyraźnie wskazują, że mimo spadku liczby przeprowadzanych kontroli wyraźnie rośnie kwota dodatkowego przypisu/odpisu będącego skutkiem przeprowadzonej kontroli.

Tego typu przykłady można mnożyć; chodzi chociażby o kary związane z naruszeniem regulacji dotyczących ochrony danych osobowych, o czym mowa była już wcześniej, czy o wzmożoną aktywność sądów rejestrowych wszczynających postępowania przymuszające do złożenia sprawozdań finansowych do repozytorium dokumentów finansowych.

Należy również zauważyć, że postępująca informatyzacja i digitalizacja ułatwia organom państwa coraz bardziej skuteczną egzekucję stosowania przepisów. W pierwszej kolejności należy tu wspomnieć o wprowadzonym jednolitym pliku kontrolnym czy obowiązku raportowania schematów podatkowych, czyli wspomnianym już MDR.

²² Dane na podstawie artykułu A. Pokojskiej z 07.05.2018 w „Dziennik Gazeta Prawna”; <https://podatki.gazetaprawna.pl/artykuly/1121615,mniej-kontroli-krajowej-administracji-skarbowej.html>.

Skomplikowanie regulacji prawnych, ich zmienność oraz wysokie zagrożenie karami czy to o charakterze karnym, czy administracyjnoprawnym (np. odpowiedzialność za naruszenie ustawy o ochronie konkurencji i konsumentów) generuje presję na kadrze zarządzającej i potęguje ryzyko związane z prowadzeniem działalności gospodarczej, jak również pełnieniem funkcji kierowniczych. Wskazać przy tym należy, że w niektórych przypadkach odpowiedzialność może dotyczyć bezpośrednio osób należących do kadry zarządzającej przedsiębiorstwem (tzw. odpowiedzialność osobista) – np. odpowiedzialność karna za nieterminowe złożenie wniosku o ogłoszenie upadłości, nieterminowe złożenie w sądzie dokumentów związanych z zamknięciem roku obrotowego, łapownictwo menedżerskie itd.

Co ważne, również w przypadku ponoszenia odpowiedzialności przez samą spółkę i nałożenia na nią kary za naruszenie przepisów, kodeks spółek handlowych umożliwia dochodzenie od członka zarządu lub członków rady nadzorczej naprawienia szkody²³. Powyższa regulacja jest dobrym przykładem konstrukcji odpowiedzialności kadry kierowniczej spółki. Zwraca uwagę, że odpowiedzialność odszkodowawcza jest uzależniona od winy członków zarządu lub członków rady nadzorczej, a jej brak powoduje wyłączenie odpowiedzialności. Nie jest to jedyna regulacja tego typu. Tytułem przykładu można wskazać również ustawę o ochronie konkurencji i konsumentów, zgodnie z którą Prezes UOKiK może nałożyć grzywnę do 2 mln złotych na osobę zarządzającą przedsiębiorstwem, jeżeli ta osoba umyślnie dopuściła do naruszenia przez przedsiębiorcę między innymi zakazów określonych w art. 6 ust. 1 pkt 1–6 ustawy²⁴.

²³ Zgodnie z art. 293 ksh dotyczącym spółki z o.o. członek zarządu, rady nadzorczej, komisji rewizyjnej oraz likwidator odpowiada wobec spółki za szkodę wyrządzoną działaniem lub zaniechaniem sprzecznym z prawem lub postanowieniami umowy spółki, chyba że nie ponosi winy. Art. 483 ksh reguluje tę kwestię analogicznie w odniesieniu do spółki akcyjnej.

²⁴ Art. 106a ustawy o ochronie konkurencji i konsumentów.

W tym kontekście warto również zwrócić uwagę na fakt, że przepisy prawa karnego oraz karnoskarbowego przewidują pewne typy czynów, sprowadzające się do braku należytego sprawowania funkcji nadzorczych²⁵. Kodeks karnoskarbowy wyraźnie wskazuje, że za przestępstwa skarbowe lub wykroczenia skarbowe odpowiada, jak sprawca, także ten, kto na podstawie przepisu prawa, umowy lub faktycznego wykonywania zajmuje się sprawami gospodarczymi, w szczególności finansowymi, osoby prawnej albo jednostki organizacyjnej niemającej osobowości prawnej. Jest to przepis, który wprost daje podstawę do odpowiedzialność kadry zarządzającej.

Warto również zauważyć, że część przestępstw może być popełniona wyłącznie umyślnie²⁶. Ważna jest przy tym kodeksowa definicja umyślności, bowiem zgodnie z przepisami prawa karnego i karnoskarbowego może ona przybrać dwie postacie:

- zamiar bezpośredni (sprawca ma zamiar popełnienia czynu, to jest chce go popełnić) albo
- zamiar ewentualny (sprawca przewiduje możliwość popełnienia czynu i na to się godzi)²⁷.

Oznacza to, że jest możliwe umyślne popełnienie czynu zabronionego tylko z tego powodu, że sprawca godzi się na popełnienie czynu, mimo iż do popełnienia czynu nie dąży.

²⁵ Np. art. 84 kks: Kto, nie dopełniając obowiązku nadzoru nad przestrzeganiem reguł obowiązujących w działalności danego przedsiębiorcy lub innej jednostki organizacyjnej, dopuszcza, chociażby nieumyślnie, do popełnienia czynu zabronionego określonego w rozdziale 6, podlega karze grzywny za wykroczenie skarbowe.

²⁶ Przestępstwo można popełnić nieumyślnie, jeżeli ustawa wyraźnie tak stanowi.

²⁷ Art. 4 kks oraz art. 9 kk.

Wdrożenie i stosowanie CMS może mieć znaczenie w kontekście oceny stopnia zawinienia kadry zarządzającej w sytuacji naruszeń. Powyższe dotyczy zarówno odpowiedzialności cywilnoprawnej, jak i karnej (karnoskarbowej). Stosowanie CMS może mieć znaczenie również przy określaniu wysokości wymierzanych kar administracyjnych.

4.4. Wzrost znajomości prawa

Kolejną przyczyną wzrostu zainteresowania compliance jest coraz większa znajomość prawa przez kadry zarządzające, a co za tym idzie – rosnąca świadomość odpowiedzialności związanej z pełnieniem funkcji kierowniczych.

W tym kontekście warto zauważyć, że wzrasta świadomość, iż często nawet z pozoru drobne zaniechania mogą prowadzić do odpowiedzialności osobistej kadry zarządzającej. Przykładem dobrze ilustrującym niewielkie niedopatrzenie i jego dalsze konsekwencje jest odpowiedzialność za brak terminowego złożenia w sądzie rejestrowym sprawozdania finansowego.

4.5. Wymóg prawny – tendencje ustawodawcze

Do wzrostu znaczenia compliance w Polsce w ostatnich latach przyczynił się projekt nowelizacji ustawy o odpowiedzialności podmiotów zbiorowych za czyny zabronione pod groźbą kary. Według projektu brak posiadania systemu zarządzania compliance stanowił przesłankę świadcząca o braku dochowania należytej staranności, co w konsekwencji mogło prowadzić do nałożenia na podmiot zbiorowy kary²⁸. Mając na uwadze powyższe, można stwierdzić, że uchwalenie projektu ustawy doprowadziłoby

²⁸ Jeżeli w VIII kadencji Sejmu projekt nie zostanie przegłosowany, to ze względu na zasadę dyskontynuacji prac Sejmu, aby doszło do uchwalenia wspomnianego projektu ustawy, projekt będzie musiał zostać ponownie przedłożony.

w konsekwencji do konieczności wdrażania systemów zarządzania compliance w większości średnich przedsiębiorstw.

Powyższa regulacja miałaby w praktyce wyjątkowy charakter, ponieważ w aktualnie obowiązującym porządku prawnym w Polsce nie funkcjonują przepisy, za wyjątkiem regulacji sektorowych dotyczących wybranych grup przedsiębiorców²⁹, które wymuszają wprowadzenie i stosowanie CMS.

4.6. Globalizacja i ujawniane afery

Jak już wspomniano, compliance jest zjawiskiem, które wywodzi się z amerykańskiego modelu prawnego i biznesowego. Pogłębiająca się globalizacja, a co za tym idzie – relacje z przedsiębiorstwami zagranicznymi – często niosą ze sobą konieczność posiadania systemu zarządzania compliance. Brak wdrożonego CMS może być w relacjach biznesowych kryterium dyskwalifikującym w pozyskiwaniu kontrahentów zagranicznych.

Niebagatelne znaczenie dla rozwoju compliance mają afery ujawniane w ostatnich latach, jak na przykład afera w grupie Volkswagen dotycząca stosowania oprogramowania pozwalającego na manipulację wynikami pomiarów emisji. Przedsiębiorstwa, w których doszło do nadużyć, próbują odzyskać utracone zaufanie klientów między innymi poprzez wdrażanie systemów zarządzania compliance. Ogromne kary nakładane na podmioty dopuszczające się naruszeń oraz milionowe roszczenia odszkodowawcze klientów stanowią nadto doskonałą zachętę do wprowadzania systemów zapewniających zgodność z prawem i etyką.

²⁹ Np. art. 9c ustawy z dnia 29 sierpnia 1997 r. Prawo bankowe (t.j. Dz.U. z 2018 r. poz. 2187 z późn. zm.).

5. Compliance – aktualny stan. Raport

Compliance w Polsce

Rosnąca rola compliance w Polsce przyniosła ze sobą pierwsze analizy dotyczące rozpowszechnienia znajomości tego terminu, stosowania systemów zarządzania zgodnością, jak również motywów ich niewprowadzania. Pierwsza tego typu analiza została przeprowadzona w 2018 r., a jej efektem jest Raport Compliance w Polsce³⁰.

Zgodnie z raportem aż w 65% badanych przedsiębiorstwach działa CMS lub jego elementy. W części przedsiębiorstw oprócz CMS są stosowane również inne systemy, np. instytucjonalna kontrola wewnętrzna czy zarządzanie ryzykiem operacyjnym. Compliance to dosyć nowa dziedzina. Fakt ten znalazł odzwierciedlenie w odpowiedzi na pytanie, jak długo w przedsiębiorstwach działa już CMS. W 17% przedsiębiorstw działa on krócej niż rok, a w 47% przedsiębiorstw CMS funkcjonuje od roku do 6 lat. Z kolei jedynie w 28% przedsiębiorstw CMS funkcjonuje powyżej 6 lat.

Ciekawie przedstawiają się również przyczyny niewprowadzenia do tej pory CMS:

- w 28% przedsiębiorstw przyczyną był brak wiedzy o tego rodzaju systemie;
- w 23% przypadków stwierdzono, że CMS nie jest konieczny ze względu na rozmiar przedsiębiorstwa lub przedmiot jego działalności;

³⁰ Raport Compliance w Polsce został przygotowany przez Instytut Compliance we współpracy z Uniwersytetem Europejskim Viadrina, EY oraz Wolters Kluwer. Wyniki zostały opracowane przez prof. dr. Bartosza Makowicza. Raport jest dostępny na stronie internetowej: <http://instytutcompliance.pl/wp-content/uploads/2018/02/RaportInstytutCompliance2018.pdf> (data dostępu: 2 września 2019 r.).

- 8% przedsiębiorstw wskazało, że CSM stanowi ciężar i może spowalniać prowadzenie biznesu;
- 21% badanych wskazało, że jest w trakcie wdrażania CMS.

Z kolei jako dwie główne przyczyny wdrożenia CMS w przedsiębiorstwach zostały wskazane bezpieczeństwo zarządu firmy oraz narzucenie takiego wymogu przez zagraniczną spółkę-matkę.

Raport wyraźnie potwierdza, że compliance w polskim biznesie jest rozumiane szeroko i dotyczy zarówno zgodności z prawem, standardami etycznymi, pozaprawnymi normami (np. ISO), jak i wymaganiami stawianymi przez kontrahentów.

Badane przedsiębiorstwa zostały zapytane również o koszty wprowadzenia CMS. Niestety wydaje się, że wyniki nie są w tym zakresie konkluzywne, bowiem aż 75% badanych albo nie znało danych w tym zakresie albo odmówiło udzielenia odpowiedzi. Pozostałe odpowiedzi wykazują ogromną rozbieżność, tj. od kosztów poniżej 5 tys. złotych aż do przekraczających 100 tys. złotych.

Badanie obejmowało również szereg kwestii dotyczących między innymi zgłaszania naruszeń w przedsiębiorstwach (ang. *wistleblowing*), osoby *compliance oficera*, jego roli i pozycji w strukturze przedsiębiorstw czy środków stosowanych w celu zapewnienia zgodności i elementów składających się na CMS. Analiza wyników prowadzi do wniosku, że znajomość i praktyczne stosowanie systemu zgodności w Polsce są „dość mocno rozpowszechnione wśród działających w Polsce przedsiębiorstw, i to nie tylko tych, w których dominuje kapitał zagraniczny. Te firmy natomiast, które CMS wdrożyły, obrały ogólnie przyjęte elementy, takie jak analiza ryzyka, podnoszenie świadomości pracowników przez szkolenia i inne działania promujące świadomość i kulturę compliance, czy w końcu

31

stosowanie odpowiednich środków reakcji na wykryte nieprawidłowości, jako punkt wyjścia działań compliance w organizacji”³¹.

Wyniki raportu wyraźnie wskazują, że przedsiębiorstwa posiadające system zarządzania zgodnością, a przynajmniej jego elementy, nie są ewenementem na rynku polskim, a kadra kierownicza coraz częściej świadomie zarządza compliance w przedsiębiorstwach³².

³¹ Prof. dr Bartosz Makowicz, z podsumowania raportu Compliance w Polsce.

³² Zwracam uwagę na fakt, że wg raportu jedną z głównych przyczyn niestosowania CMS jest brak takiej potrzeby. Oznacza to, że dane przedsiębiorstwo dokonało świadomej analizy potrzeb i ryzyk.

Rozdział 2. Aktualne tendencje ustawodawcze regulujące compliance w Polsce

Łukasz Napiórkowski

W rozdziale pierwszym ukazano znaczenie systemu zgodności, omówiono obszary jego stosowania oraz ryzyka związane z niedochowaniem compliance (non-compliance). Wykazano również pozytywny wpływ działań systemu na organizacje, efekty dobrowolnego przyjęcia przez nie pewnych standardów i zobowiązań, jak również coraz większe zainteresowanie samym zagadaniem wśród zarządzających przedsiębiorstwami.

Nie sposób jednak pominąć zainteresowania tematyką compliance także wśród ustawodawców oraz organów nadzorczych poszczególnych państw i instytucji międzynarodowych, w tym unijnych³³. Prawodawcy z jednej strony nakładają na przedsiębiorców obowiązki samoregulacyjne, które mają zapewnić zgodność z prawem działań prowadzonych w organizacji, z drugiej zaś – wprowadzają uprawnienia i obowiązki po stronie organów państwa sprawujących kontrolę nad działaniami tychże przedsiębiorców.

³³ Jest to spowodowane doświadczeniami z przeszłości, czyli aktami korupcji oraz naruszania zasad uczciwej konkurencji. Wystarczy wspomnieć w tym miejscu takie wydarzenia, jak afery Watergate, Panama Papers czy Ivana Fredericka Boesky'ego w Stanach Zjednoczonych, czy tzw. czarne kasy Siemensu bądź pranie rosyjskich pieniędzy w estońskich oddziałach Danske Bank.

Organy kontrolne mogą coraz częściej sankcjonować działalność non-compliance poprzez nakładanie dotkliwych kar na podmioty gospodarcze, a nawet na członków ich organów.

Coraz większa liczba regulacji wprowadzanych zarówno na szczeblu międzynarodowym, jak i krajowym powoduje, że już nie tylko duże zagraniczne organizacje działające w Polsce mają działy dedykowane obszarowi compliance. Również rodzimi przedsiębiorcy, w tym mali i średni, z każdym rokiem coraz częściej decydują się na wprowadzenie przynajmniej stanowiska tzw. compliance oficera.

Wzmoczone działania w zakresie compliance, które mogliśmy dotychczas zaobserwować u polskiego prawodawcy, obejmują w szczególności rynek finansowy. Tytułem przykładu można wymienić np. rozporządzenie Ministra Rozwoju i Finansów z dnia 6 marca 2017 r. w sprawie systemu zarządzania ryzykiem i systemu kontroli wewnętrznej, polityki wynagrodzeń oraz szczegółowego sposobu szacowania kapitału wewnętrznego w banku³⁴ czy też rozporządzenie Ministra Finansów z dnia 29 maja 2018 r. w sprawie szczegółowych warunków technicznych i organizacyjnych dla firm inwestycyjnych, banków, o których mowa w art. 70 ust. 2 ustawy o obrocie instrumentami finansowymi, i banków powierniczych³⁵. W obu tych rozporządzeniach wprowadzono m.in. tryb anonimowego zgłaszania naruszeń prawa oraz obowiązujących w banku procedur i standardów etycznych. Objęcie sektora bankowego obowiązkiem posiadania odpowiednich procedur jest uzasadnione skalą działania i zagrożeń. Faktem jednak jest to, że wskazane regulacje obejmują dosyć wąski krąg organizacji.

³⁴ Dz.U. z 2017 r. poz. 637.

³⁵ Dz.U. z 2018 r. poz. 1111

Konieczność wprowadzenia odpowiednich przepisów odnoszących się już do szerszego grona podmiotów gospodarczych zostało przewidziane w Rządowym Programie Przeciwdziałania Korupcji na lata 2018–2020³⁶.

W planie realizacji tego programu przewidziano m.in.:

- wzmocnienie regulacji dotyczących odpowiedzialności karnej podmiotów zbiorowych poprzez opracowanie projektu ustawy o zmianie ustawy o odpowiedzialności podmiotów zbiorowych za czyny zabronione pod groźbą kary oraz przeprowadzenie w tym zakresie procesu legislacyjnego;
- stworzenie jednolitego systemu przepisów eliminujących możliwość powstawania stosunku podległości służbowej pomiędzy członkami rodziny w instytucjach wydatkujących środki publiczne poprzez przygotowanie i przeprowadzenie rządowego procesu legislacyjnego projektu ustawy o jawności życia publicznego (z przewidzianym terminem realizacji do 31 grudnia 2020 r.).

Na szczeblu międzynarodowym również widzimy bardzo wzmożoną tendencję do regulacji zagadnień compliance, które ostatecznie również mają wpływ na polskie ustawodawstwo.

Obecnie dużą część polskich przedsiębiorców zмага się z obowiązkami nałożonymi przepisami ustawy z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu³⁷. Ustawa ta stanowi implementację dyrektywy Parlamentu Europejskiego i Rady (UE) 2015/849 z dnia 20 maja 2015 r. w sprawie zapobiegania wykorzystywaniu systemu finansowego do prania pieniędzy lub finansowania terroryzmu, zmieniająca rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 648/2012

³⁶ Uchwała nr 207 Rady Ministrów z dnia 19 grudnia 2017 r. w sprawie Rządowego Programu Przeciwdziałania Korupcji na lata 2018–2020 (M. P. z 2018 r. poz. 12 z późn. zm.).

³⁷ Tekst jednolity Dz.U. z 2019 r. poz. 1115 z późn. zm.

i uchylająca dyrektywę Parlamentu Europejskiego i Rady 2005/60/WE oraz dyrektywę Komisji 2006/70/WE (tj. tzw. „dyrektywy AML IV”). Polska ustawa zdecydowanie poszerzyła katalog instytucji zobowiązanych³⁸ do przestrzegania jej stosowania (m.in. o podmioty świadczące usługi dla spółek i trustów czy podmioty świadczące usługi w zakresie wymiany pomiędzy walutami wirtualnymi a środkami płatniczymi). Jednocześnie nałożono nią szereg nowych obowiązków na wspomniane instytucje zobowiązane, w tym obowiązek zgłaszania informacji o beneficjentach rzeczywistych do Centralnego Rejestru Beneficjentów Rzeczywistych.

Wdrożenie dyrektywy AML IV zajęło polskiemu ustawodawcy bardzo dużo czasu, gdyż w założeniu państwa członkowskie Unii Europejskiej miały obowiązek wdrożyć ją do dnia 26 czerwca 2017 r. Natomiast w kolejce stoją już kolejne wyzwania w zakresie compliance. Nasz rodzimy ustawodawca musi bowiem w najbliższym czasie dokonać transpozycji m.in.:

- dyrektywy w sprawie ochrony osób zgłaszających przypadki naruszenia prawa Unii, którą Rada Unii Europejskiej zatwierdziła 7 października 2019 r. (tj. tzw. „dyrektywy o ochronie sygnalistów”) oraz
- dyrektywy Parlamentu Europejskiego i Rady (UE) 2018/1673 z dnia 23 października 2018 r. w sprawie zwalczania prania pieniędzy za pomocą środków prawnych (tj. tzw. „dyrektywy AML VI”).

Polska jest zobowiązana do wprowadzenia w życie przepisów ustawowych, wykonawczych i administracyjnych niezbędnych do transpozycji pierwszej ze wspomnianych dyrektyw najpóźniej do dnia 15 maja 2021 r. W przypadku dyrektywy AML VI termin jest jeszcze krótszy i mija już 3 grudnia 2020 r.

³⁸ Katalog instytucji zobowiązanych znajduje się w przepisie art. 2 ust. 1 ustawy z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu.

W dalszej części rozdziału przybliżono planowane inicjatywy ustawodawcze w zakresie compliance oraz założenia dyrektywy AML VI. Tematyka dyrektywy w sprawie ochrony osób zgłaszających przypadki naruszenia prawa Unii zostanie omówiona kompleksowo w rozdziale 3 niniejszego opracowania.

1. Założenia dyrektywy AML VI

Dyrektywa Parlamentu Europejskiego i Rady (UE) 2018/1673 z dnia 23 października 2018 r. w sprawie zwalczania prania pieniędzy za pomocą środków prawnokarnych w swoim założeniu ma uzupełnić i poprawić stosowanie dyrektywy AML IV. Ma to zostać osiągnięte m.in. poprzez wprowadzenie skuteczniejszej i szybszej współpracy transgranicznej między właściwymi organami.

Jednocześnie niniejsza dyrektywa ustanawia dodatkowe wymogi dotyczące kryminalizacji przestępstwa prania pieniędzy i pociąga daleko idące skutki nie tylko dla popełniających je osób fizycznych, ale również dla osób prawnych zaangażowanych w proceder.

W dyrektywie AML VI przyjęto jednolite definicje kategorii „działalności przestępczej”, obejmującej przestępstwa źródłowe w stosunku do prania pieniędzy, „mienia” oraz „osoby prawnej”.

Definicja działalności przestępczej na gruncie dyrektywy obejmuje wszelkiego rodzaju przestępczy udział w popełnieniu przestępstwa, który zgodnie z prawem krajowym jest zagrożony:

- karą pozbawienia wolności lub aresztu maksymalnie na więcej niż rok,
lub

- w stosunku do których dolna granica zagrożenia karą jest wyższa niż sześć miesięcy pozbawienia wolności lub aresztu (w przypadku, gdy system prawny państwa członkowskiego określa w odniesieniu do przestępstw minimalny próg zagrożenia karą).

Postanowiono jednak również wprowadzić otwarty katalog przestępstw uznawanych w każdym przypadku za działalność przestępczą. Katalog ten obejmuje m.in. udział w zorganizowanej grupie przestępczej i wymuszenia, terroryzm, handel ludźmi i przemyt nielegalnych migrantów, nielegalny handel narkotykami i substancjami psychotropowymi, korupcję, oszustwa, ale też przestępstwa podatkowe odnoszące się do podatków bezpośrednich i pośrednich (określonych w prawie krajowym), wykorzystywanie informacji wewnętrznych i manipulacja na rynku oraz cyberprzestępstwa. Pełny wykaz działalności przestępczej został wymieniony w artykule 2 ust. 1 dyrektywy AML VI.

Przepisy dyrektywy zobowiązują dodatkowo państwa członkowskie do zapewnienia, aby niektóre rodzaje prania pieniędzy były zagrożone karą również w przypadku, gdy zostaną popełnione przez sprawcę działalności przestępczej, z której pochodzi to mienie. Chodzi zatem o ukaranie podmiotu, który pierze pieniądze, które wcześniej uzyskał w sposób przestępny. Wobec powyższego przepisami dyrektywy zdecydowano się objąć karą przestępstwa prania pieniędzy polegające na konwersji lub przekazaniu mienia pochodzącego z działalności przestępczej, ukryciu lub zatajeniu prawdziwego pochodzenia takiego mienia oraz nabyciu, posiadaniu albo użytkowaniu mienia, ze świadomością w momencie jego otrzymania, że pochodziło ono z działalności o charakterze przestępczym. Dyrektywa zobowiązuje również do penalizacji, czyli uznania za przestępstwo, czynów pomocnictwa, podżegania i usiłowania popełnienia przestępstwa prania pieniędzy określonego powyżej.

Jednocześnie państwowom wdrażającym dyrektywę AML VI pozostawiono możliwość ukarania sprawcy powyższych czynów prania pieniędzy, jeżeli sprawca podejrzewał lub powinien był wiedzieć, że mienie pochodzi z działalności o charakterze przestępczym. W tym przypadku mamy zatem do czynienia z możliwością ukarania podmiotu z uwagi na lekkomyślność lub niedbalstwo.

Na gruncie dyrektywy AML VI zdecydowano się również objąć osoby prawne karą za którekolwiek z przestępstw prania pieniędzy, o których mowa powyżej, popełnione w celu przysporzenia im korzyści przez dowolne osoby, działające indywidualnie lub jako część organu tej osoby prawnej zajmującej ważną pozycję w jej strukturze, opierając się na którymkolwiek z następujących elementów:

- prawo reprezentowania osoby prawnej,
- upoważnienie do podejmowania decyzji w imieniu osoby prawnej, lub
- upoważnienie do sprawowania kontroli w ramach danej osoby prawnej.

Co więcej przewiduje się możliwość pociągnięcia osób prawnych do odpowiedzialności również z uwagi na brak nadzoru lub kontroli, gdy osoba podległa osobie zajmującej ważną pozycję w strukturze osoby prawnej popełni jedno z wcześniej opisanych przestępstw na korzyść osoby prawnej.

Celem jednolitego karania przestępstwa prania pieniędzy w całej Unii Europejskiej zdecydowano się, aby opisane wyżej przestępne czyny były zagrożone maksymalną karą pozbawienia wolności w wymiarze co najmniej 4 lat. Państwa członkowskie zostały zobowiązane do wprowadzenia dodatkowych kar lub środków, takich jak m. in. grzywny, czasowe lub stałe odcięcie dostępu do finansowania publicznego, w tym do procedur przetargowych, dotacji i koncesji, tymczasowe zakazy prowadzenia działalności handlowej lub tymczasowe zakazy ubiegania się o wybieralne lub publiczne stanowisko.

Jednolita unijna penalizacja poszczególnych przestępstw prania pieniędzy oraz przewidziane dotkliwe sankcje powodują, że przedsiębiorcy będą musieli bacznie przyglądać się ruchom polskiego ustawodawcy w zakresie wdrożenia dyrektywy AML VI. Pozostawione stosunkowo małe pole do odmiennej regulacji omówionych zagadnień umożliwi natomiast odpowiednio wczesne przygotowanie się na czekające nas zmiany. Wcześniejsze zainteresowanie się tym tematem zyskuje na doniosłości, gdy zdamy sobie sprawę z tego, że polski ustawodawca wiele z obowiązków nałożonych przedmiotową dyrektywą przewidział już w projekcie nowej ustawy o odpowiedzialności podmiotów zbiorowych za czyny zabronione pod groźbą kary, której projekt w chwili powstawania niniejszej publikacji znajdował się w Sejmie RP.

2. Projekt nowej ustawy o odpowiedzialności podmiotów zbiorowych za czyny zabronione pod groźbą kary

Nowa ustawa ma zastąpić dotychczas obowiązującą z dnia 28 października 2002 r. o odpowiedzialności podmiotów zbiorowych za czyny zabronione pod groźbą kary³⁹.

Odpowiedzialność wynikająca z przepisów nowego aktu prawnego jest kwestią istotną i obejmuje w swoim założeniu bardzo dużą liczbę podmiotów. Pod pojęciem podmiotu zbiorowego należy bowiem rozumieć osobę prawną oraz jednostki organizacyjne niemające osobowości prawnej, którym odrębne przepisy przyznają zdolność prawną, z wyłączeniem

³⁹ Ustawa z dnia 28 października 2002 r. o odpowiedzialności podmiotów zbiorowych za czyny zabronione pod groźbą kary (t.j. Dz.U. z 2019 r. poz. 628 z późn. zm.).

Skarbu Państwa, jednostek samorządu terytorialnego i ich związków; jak również spółkę handlową z udziałem Skarbu Państwa, jednostki samorządu terytorialnego lub związku takich jednostek; spółkę kapitałową w organizacji; podmiot w stanie likwidacji oraz przedsiębiorcę niebędącego osobą fizyczną; a także zagraniczną jednostkę organizacyjną (art. 2).

Katalog podmiotów zbiorowych jest zatem bardzo szeroki. Odwołuje się on bowiem do cywilistycznego pojęcia „osoby prawnej”. Zgodnie z przepisem art. 33 Kodeksu cywilnego osobami prawnymi Skarb Państwa i jednostki organizacyjne, którym przepisy szczególne przyznają osobowość prawną⁴⁰. W świetle takiej definicji należy uznać, że obecnie obowiązująca ustawa z dnia 28 października 2002 r. obejmuje swoim zakresem podmiotowym, m.in. wszystkie spółki prawa handlowego, ale też przedsiębiorstwa państwowe, fundacje, wspólnoty mieszkaniowe i wiele innych.

Dotychczasowe brzmienie ustawy uzależnia jednak odpowiedzialność podmiotu zbiorowego od uprzedniego ukarania osoby fizycznej, działającej w jej imieniu, za zachowanie przestępne.

Jak wynika z brzmienia przepisu art. 3 dotychczasowej ustawy, podmiot zbiorowy podlega odpowiedzialności za czyn zabroniony, którym jest zachowanie osoby fizycznej:

1. działającej w imieniu lub w interesie podmiotu zbiorowego w ramach uprawnienia lub obowiązku do jego reprezentowania, podejmowania w jego imieniu decyzji lub wykonywania kontroli wewnętrznej albo przy przekroczeniu tego uprawnienia lub niedopełnieniu tego obowiązku;
2. dopuszczonej do działania w wyniku przekroczenia uprawnień lub niedopełnienia obowiązków przez osobę, o której mowa w pkt 1;

⁴⁰ Art. 33 ustawy z dnia 23 kwietnia 1964 r. Kodeks cywilny (t.j. Dz.U. z 2019 r. poz. 1145).

3. działającej w imieniu lub interesie podmiotu zbiorowego, za zgodą lub wiedzą osoby, o której mowa w pkt. 1;
 4. będącej przedsiębiorcą, który bezpośrednio współdziała z podmiotem zbiorowym w realizacji celu prawnie dopuszczalnego;
- jeżeli zachowanie to przyniosło lub mogło przynieść podmiotowi zbiorowemu korzyść, chociażby niemajątkową.

Natomiast art. 4 ustawy z dnia 28 października 2002 r. wskazuje na akcesoryjność odpowiedzialności podmiotu zbiorowego. Zgodnie z jego brzmieniem, aby można było ukarać podmiot zbiorowy, najpierw osoba fizyczna dopuszczająca się naruszeń musi zostać prawomocnie skazana. To natomiast powoduje, że mimo iż obecna ustawa reguluje w znacznym stopniu zasady odpowiedzialności podmiotów zbiorowych za czyny zabronione pod groźbą kary jako przestępstwa lub przestępstwa skarbowe oraz zasady postępowania w przedmiocie takiej odpowiedzialności, to jednak z uwagi na konieczność przypisania odpowiedzialności za popełnienie sankcjonowanych ustawą czynów konkretnej osobie fizycznej, według projektodawców i orędowników jej zmiany, jest ona zwyczajnie nieefektywna.

Przy obecnie złożonych strukturach organizacyjnych, gdzie proces decyzyjny nierzadko nie jest uzależniony od konkretnej osoby fizycznej, można zrozumieć taki argument. Projektodawcy w uzasadnieniu do projektu nowej ustawy o odpowiedzialności podmiotów zbiorowych za czyny zabronione pod groźbą kary przytaczają statystyki wskazujące na znikomą efektywność obecnych regulacji⁴¹.

⁴¹ Projekt ustawy wraz z uzasadnieniem: [http://orka.sejm.gov.pl/Druki8ka.nsf/Projekty/8-020-1211-2019/\\$file/8-020-1211-2019.pdf](http://orka.sejm.gov.pl/Druki8ka.nsf/Projekty/8-020-1211-2019/$file/8-020-1211-2019.pdf), dostęp: 17 września 2019 r.

Liczba spraw, które wpłynęły do sądów w latach 2013–2017:

- w 2013 r. – 26 spraw,
- w 2014 r. – 31 spraw,
- w 2015 r. – 14 spraw,
- w 2016 r. – 25 spraw,
- w 2017 r. – 14 spraw.

Jednocześnie przy znikomej liczbie spraw również wymierzane kary były bardzo niskie. Większość z nich jest bliska dolnej granicy wymiaru określonej na 1000 złotych. Może się to wydawać zaskakujące, gdyż obecna ustawa przewiduje możliwość wymierzenia bardzo wysokiej kary pieniężnej oraz przepadku przedmiotów lub korzyści związanych z popełnieniem czynu zabronionego. Górny wymiar kary może wynieść nawet 5 000 000 złotych, przy czym ustawodawca przyjął, że kara nie może przekroczyć 3% wysokości przychodu osiągniętego przez podmiot zbiorowy w roku obrotowym, w którym popełniono czyn zabroniony będący podstawą jego odpowiedzialności. Orzekanie niskich kar wskazuje zatem nie na czyny o niewielkim znaczeniu, a w głównej mierze na to, że kary są wymierzane w stosunku do małych podmiotów zbiorowych. Konkluzją tego jest to, że obecne regulacje nie zapewniają dostatecznych narzędzi do walki z dużymi podmiotami naruszającymi przepisy. Projektowana ustawa ma temu zaradzić poprzez odejście od zasady akcesoryjności i wprowadzenie winy w organizacji.

Zmiany są podyktowane również zobowiązaniami międzynarodowymi Polski wynikającymi z dokumentów prawnych przyjętych przez Unię Europejską, Radę Europy i Organizację Współpracy Gospodarczej i Rozwoju (OECD). Polska chcąc się zastosować do nałożonych na nią obowiązków, jest zobowiązana do wdrożenia sprawnie działającego systemu

odpowiedzialności osób prawnych za działania na szkodę finansów Unii Europejskiej czy podejmujących czynności o charakterze korupcyjnym⁴².

2.1. Podstawowe założenia projektowanej ustawy

Nowa ustawa o odpowiedzialności podmiotów zbiorowych za czyny zabronione pod groźbą kary ma zdecydowanie usprawnić działania wobec podmiotów zbiorowych. Jednocześnie ma wprowadzić szereg nowych rozwiązań rozszerzających odpowiedzialność za działania ich pełnomocników, pracowników, współpracowników, podwykonawców, kontrahentów i ich pracowników.

Podstawowe założenia nowej ustawy można ująć w 4 punktach, tj.:

- poszerzenie podstaw odpowiedzialności podmiotów zbiorowych poprzez wprowadzenie winy w organizacji – uznanie działania lub zaniechania podmiotów działających w imieniu podmiotu zbiorowego za własne zachowania podmiotu zbiorowego;
- poszerzenie odpowiedzialności podmiotu zbiorowego o wszystkie czyny zabronione pod groźbą kary jako przestępstwo lub przestępstwo skarbowe, z wyłączeniem przestępstw prywatnoskargowych;
- odejście od zasady uprzedniego uzyskania prejudykatu, czyli uprzedniego skazania osoby fizycznej działającej w imieniu podmiotu zbiorowego;
- zagwarantowanie ochrony sygnalistom zgłaszającym informacje o nieprawidłowościach w podmiocie zbiorowym.

⁴² Por. np. zobowiązania wynikające z dyrektywy Parlamentu Europejskiego i Rady 2017/1371/UE z dnia 5 lipca 2017 r. w sprawie zwalczania za pośrednictwem prawa karnego nadużyć na szkodę interesów finansowych Unii.

2.2. Rozszerzenie katalogu podmiotowego ustawy poprzez zastosowanie ustawy do zagranicznych podmiotów zbiorowych

Projektowana ustawa przewiduje dosyć podobną do dotychczasowej definicję podmiotu zbiorowego. Zdecydowano się jednak rozszerzyć jej stosowanie na podmioty, które nie posiadają siedziby na terytorium RP, ale prowadzą działalność na jej terenie. Wobec tego przepisy ustawy mają znaleźć zastosowanie nie tylko do podmiotu zbiorowego posiadającego siedzibę w Polsce, bez względu na miejsce popełnienia czynu zabronionego, ale również do podmiotu mającego siedzibę lub prowadzącego działalność za granicą, jeżeli czyn zabroniony będący podstawą odpowiedzialności został popełniony na terytorium Rzeczypospolitej Polskiej lub skutek stanowiący jego znamię wystąpił na jej terytorium, lub czyn był skierowany przeciwko jej interesom lub interesom obywatela polskiego, polskiej osoby prawnej lub polskiej jednostki organizacyjnej niemającej osobowości prawnej⁴³.

2.3. Czym jest czyn zabroniony w świetle nowej ustawy?

W projekcie ustawy przyjmuje się nową definicję czynu zabronionego rozumianego jako przestępstwo ścigane z oskarżenia publicznego lub jako przestępstwo skarbowe, z wyłączeniem czynów popełnionych przez opublikowanie materiału prasowego oraz innych naruszeń praw związanych z przekazywaniem myśli ludzkiej, do których stosuje się przepisy o odpowiedzialności prawnej i postępowaniu w sprawach

⁴³ Art. 3 ust. 2. Projektu ustawy o odpowiedzialności podmiotów zbiorowych za czyny zabronione pod groźbą kary; Projekt ustawy wraz z uzasadnieniem: [http://orka.sejm.gov.pl/Druki8ka.nsf/Projekty/8-020-1211-2019/\\$file/8-020-1211-2019.pdf](http://orka.sejm.gov.pl/Druki8ka.nsf/Projekty/8-020-1211-2019/$file/8-020-1211-2019.pdf), dostęp: 17 września 2019 r.

prasowych określone w ustawie z dnia 26 stycznia 1984 r. – Prawo prasowe (Dz.U. z 2018 r. poz. 1914)⁴⁴.

W swojej istocie postanowiono zatem odejść od obecnie obowiązującego zamkniętego katalogu czynów zabronionych⁴⁵, opowiadając się za zasadą powszechnej odpowiedzialności podmiotów zbiorowych. Przy czym należy zauważyć, że projektodawca skupia się na czynach będących przestępstwem ściganym z oskarżenia publicznego i przestępstwach skarbowych, a zatem zrezygnował z objęcia nową ustawą czynów stanowiących wykroczenia, przestępstwa prywatnoskargowe, ale również stanowiące tzw. przestępstwa prasowe.

2.4. Jaka odpowiedzialność za czyn zabroniony?

Projektodawca oparł odpowiedzialność podmiotu zbiorowego na dwóch zasadach – odpowiedzialności za czyny własne podmiotu zbiorowego oraz odpowiedzialności za czyny popełnione przez osoby fizyczne pozostające bezpośrednio w związku z prowadzoną przez ten podmiot działalnością. Przy czym, inaczej niż w obecnie obowiązującej ustawie, odpowiedzialność tę oparto na koncepcji przypisania odpowiedzialności bezpośrednio podmiotowi zbiorowemu oraz koncepcji winy anonimowej.

Odpowiedzialność za czyny własne uregulowana w art. 5 projektowanej ustawy polega na przypisaniu winy podmiotowi zbiorowemu, gdy popełnienie czynu penalizowanego nastąpi wskutek działania lub zaniechania organu podmiotu zbiorowego albo umyślnego działania lub zaniechania członka tego organu. Co więcej podmioty zbiorowe będą odpowiadały również za działania swoich pełnomocników

⁴⁴ Art. 2 ust. 2. *Ibidem*.

⁴⁵ Art. 16 ustawy z dnia 28 października 2002 r. o odpowiedzialności podmiotów zbiorowych za czyny zabronione pod groźbą kary (t.j. Dz.U. z 2019 r. poz. 628 z późn. zm.).

(w tym prokurentów), pracowników, jak również podwykonawców oraz pracowników i osoby działające w interesie lub na rzecz jego podwykonawców. Naturalnie odpowiedzialność za podwykonawców i osoby działające w interesie lub na ich rzecz, ogranicza się jedynie do czynów, które chociażby pośrednio, spowodują uzyskanie przez podmiot zbiorowy korzyści majątkowej.

Analogicznie również w przypadku odpowiedzialności za czyny popełnione przez osoby fizyczne pozostające bezpośrednio w związku z prowadzoną przez ten podmiot działalnością, podmiot zbiorowy będzie odpowiadać za przestępstwa popełnione na jego korzyść, bez konieczności uzyskania prawomocnego skazania osoby fizycznej jako warunku wstępnego odpowiedzialności tego podmiotu. Usunięcie tej przesłanki do pociągnięcia do odpowiedzialności podmiotu zbiorowego postulowała od dawna Rada Europy, która już w 2013 r. rekomendowała wyeliminowanie prejudykatu jako warunku odpowiedzialności podmiotu zbiorowego⁴⁶. Oznacza to, że sąd orzekając w sprawie tego, czy osoba fizyczna dopuściła się przestępstwa penalizowanego projektowaną ustawą, będzie jednocześnie orzekać również w sprawie odpowiedzialności podmiotu zbiorowego. Brak przy tym wymogu ustalenia konkretnego sprawcy, tj. konkretnej osoby fizycznej, a zatem podmiot zbiorowy będzie mógł zostać ukarany, mimo anonimowości sprawcy. Oczywiście czyn zabroniony musi w takim przypadku pozostawać w bezpośrednim związku z działalnością podmiotu. Nie może bowiem dojść do sytuacji, w której podmiot zbiorowy poniesie odpowiedzialność za czyny popełnione np. przez osoby fizyczne, które całkowicie niezależnie od tego czynu realizują funkcję organu.

⁴⁶ Por. Konwencję Rady Europy z dnia 16 maja 2005 r. o praniu, ujawnianiu, zajmowaniu i konfiskacie dochodów pochodzących z przestępstwa (Dz.U. z 2008 r. poz. 1028).

W nowej ustawie przewidziano również warunki zwolnienia podmiotu zbiorowego od odpowiedzialności, o której mowa powyżej. Jak stanowi przepis art. 6 ust. 6 projektowanej ustawy, podmiot zbiorowy nie odpowiada za nieprawidłowość, jeżeli wykáže, że wszystkie organy i osoby uprawnione do działania w jego imieniu lub interesie zachowały **należyłą staranność** wymaganą w danych okolicznościach w organizacji działalności tego podmiotu oraz w nadzorze nad tą działalnością. Jako należyłą staranność w świetle ustawy należy rozumieć określony, modelowy sposób postępowania w profesjonalnym obrocie handlowym, jaki jest faktycznie i powszechnie stosowany w danej sytuacji. Przy czym należy też przypomnieć, że ustawa posługuje się także konstrukcją winy w wyborze, winy w nadzorze i winy organizacyjnej. Biorąc powyższe pod rozwagę, stanie się konieczne wprowadzanie wewnętrznych polityk należytej staranności, np. przy wyborze podwykonawcy.

Jak można zaobserwować w ostatnim czasie, polityki należytej staranności stają się coraz bardziej powszechne. Trend ten możemy zauważyć w szczególności w takiej gałęzi prawa jaką są podatki. Tam również mamy do czynienia z koniecznością udowodnienia należytej staranności m.in. przy dokonywaniu płatności na rzecz zagranicznych dostawców usług. Aby przykładowo polska spółka z ograniczoną odpowiedzialnością będąca płatnikiem mogła pobrać podatek u źródła (*withholding tax* – WHT) w niższej wysokości, musi ona z należyłą starannością zweryfikować kontrahenta. Wprowadzenie odpowiedniej polityki w zakresie WHT pozwoli zagwarantować odpowiednią kontrolę statusu kontrahenta i prawo do skorzystania z preferencyjnych stawek wynikających z właściwej umowy o unikaniu podwójnego opodatkowania, jak również z odpowiedniego zwolnienia.

Podobnie będzie to wyglądało w przypadku należytej staranności na gruncie omawianego projektu ustawy. Zweryfikowanie obecnych polityk

funkcjonujących w przedsiębiorstwie i dostosowanie ich do obowiązującego prawa będzie kluczowe dla podmiotów zbiorowych, z uwagi na przeniesienie ciężaru dowodu w przedmiocie dochowania należytej staranności na podmiot zbiorowy. Posiadanie odpowiednich regulacji pozwala nie tylko na ukształtowanie odpowiedniego zachowania i kontroli organów podmiotów zbiorowych, ale również będzie pewnym argumentem przed sądem.

2.5. Katalog kar i środków orzekanych wobec podmiotów zbiorowych

Widelki wysokości kar pieniężnych za nieprzestrzeganie przepisów ustawy przewiduje się w zakresie od 30 000 do 30 000 000 zł. Wysokość kary może być podniesiona dwukrotnie w ściśle określonych ustawą sytuacjach. Można zatem przyjąć, że najwyższą karą pieniężną jest kara 60 000 000 zł. W projekcie ustawy zrezygnowano z ograniczenia kary do 3% przychodu osiągniętego w roku obrotowym przez podmiot zbiorowy, w którym popełniono czyn zabroniony.

Mimo usunięcia wspomnianej zasady, która w swojej istocie miała dostosowywać karę do skali działalności podmiotu zbiorowego, przewidziano inne uregulowania w zakresie miarkowania kary. Zgodnie z przepisem art. 28 projektowanej ustawy sąd powinien między innymi uwzględnić sytuację majątkową podmiotu zbiorowego, wpływ ukarania na jego dalsze funkcjonowanie, a także działania podejmowane w ramach podmiotu zbiorowego po popełnieniu czynu.

Oprócz kar pieniężnych ustawa przewiduje szereg innych, z których najbardziej surową będzie rozwiązanie podmiotu zbiorowego. Kara ta będzie mogła zostać orzeczona w sytuacjach wyjątkowych, tj. tzw. „sytuacjach beznadziejnych – nie rokujących na przyszłość”, a także jedynie

pod warunkiem, że zagrożenie popełnionego czynu karą wynosić będzie co najmniej 5 lat pozbawienia wolności. Ponadto powyższa kara nie znajdzie również zastosowania do osób prawnych, o których bycie prawnym zdecydował ustawodawca, tj. podmiotów powołanych ustawą.

Inne środki, jakie będą mogły być orzeczone wobec podmiotów zbiorowych, to:

- przepadek,
- określone obowiązki,
- określone zakazy,
- nawiązka,
- podanie wyroku do wiadomości publicznej,
- czasowe zamknięcie zakładu podmiotu zbiorowego.

Wyżej wymienione środki będą mogły być stosowane do wszystkich podmiotów zbiorowych bez wyjątku.

2.6. Zalecenia dla przedsiębiorców

Nowa ustawa o odpowiedzialności podmiotów zbiorowych za czyny zabronione pod groźbą kary w obecnie projektowanym brzmieniu może stać się kluczowym aktem prawnym dotyczącym materii compliance w Polsce, któremu trzeba będzie się przyjrzeć i dostosować do jego przepisów.

Obecny projekt zakłada sześciomiesięczne *vacatio legis*. Jest to niewątpliwie okres bardzo krótki, patrząc na obowiązki nakładane na podmioty zbiorowe. Przedsiębiorcy będą musieli rozpocząć przygotowania do wprowadzenia wewnętrznych regulaminów nieco wcześniej, aby zdążyć dostosować się do tak szerokich zmian.

Polityki dotyczące zachowania należytej staranności oraz dotyczące ochrony sygnalistów zdecydowanie warto mieć i należałoby zastanowić się nad ich wprowadzeniem jeszcze przed uchwaleniem wspomnianej ustawy. Jak wykazano wcześniej, zmiany prawne w tym zakresie będą musiały zostać uchwalone – czy to w obecnym brzmieniu, czy w zmienionym – stąd warto już wcześniej zainteresować się tym tematem.

Warto przy tej okazji przytoczyć inne z pozoru błahe obowiązki nakładane na przedsiębiorców w ostatnich latach, na które można było się przygotować, a jednak historia pokazuje, że dostosowanie się do nowych przepisów zajęło podmiotom gospodarczym nieco dłużej niż powinno. Za przykład może posłużyć obowiązek opatrywania sprawozdań finansowych kwalifikowanym podpisem elektronicznym lub profilem zaufanym ePUAP. Mimo iż obowiązek ten był znany dużo wcześniej, wiele podmiotów było nieprzygotowanych do złożenia dokumentów finansowych do Repozytorium Dokumentów Finansowych po 1 października 2018 r. Efektem tego było niedochowanie ustawowego terminu do sporządzenia i złożenia dokumentów Repozytorium Dokumentów Finansowych. Elektroniczna forma składania tych dokumentów pozwala natomiast Sądowi Rejestrowemu na sprawniejsze inicjowanie postępowania przymuszającego wobec spóźnialskich podmiotów, a to często kończy się nałożeniem dotkliwej kary na przedsiębiorcę.

Innym wartym przytoczenia przykładem jest Centralny Rejestr Beneficjentów Rzeczywistych, który ruszył 13 października 2019 r. Szereg podmiotów zostało zobowiązanych do ujawnienia swojego beneficjenta rzeczywistego w terminie 7 dni od dnia dokonania wpisu danej spółki do Krajowego Rejestru Sądowego. W przypadku spółek, które są już wpisane do KRS, zgłoszenie powinno nastąpić najpóźniej do 13 kwietnia 2020 r. Niewywiązanie się przez spółkę z obowiązku zgłoszenia do rejestru zagrożone jest karą pieniężną do 1 000 000 zł. Na rynku prawniczym można

51

zaobserwować małe zainteresowanie podmiotów zobowiązanych tym obowiązkiem i to mimo dotkliwych kar. Wydaje się zatem, że zdecydowanie większe zainteresowanie tym zagadnieniem nastąpi na początku kwietnia 2020 r., gdy pozostanie już bardzo mało czasu na zidentyfikowanie beneficjenta rzeczywistego. Może się wtedy okazać, że członek zarządu, który nie dopilnuje zgłoszenia, będzie musiał głęboko sięgnąć do własnej kieszeni.

Te przykłady obrazują, jak ważne jest zachowanie compliance i odpowiednio wczesne podejmowanie zmian dostosowujących w organizacji.

Rozdział 3. Ochrona sygnalistów jako element efektywnej polityki compliance

Joanna Jurasz

1. Kim jest sygnalista i jaka jest jego rola w ujawnianiu nieprawidłowości w organizacji

W każdej organizacji, niezależnie od tego, czy jest to organizacja prywatna, czy publiczna, rozbudowana, czy o mało złożonej strukturze, może dojść do różnego rodzaju bezprawnych działań albo przypadków nadużywania prawa – czyli celowego działania bądź zaniechania skutkującego osiągnięciem korzyści przez ich sprawcę i poniesieniem straty przez ofiarę. Takie działania mogą mieć różną formę – może to być zaniechanie obowiązków, brak należytej staranności, malwersacje, nadużycia finansowe, mobbing, ale także ustawianie przetargów, kradzież własności intelektualnej, niewłaściwe rozliczanie czy fałszowanie wydatków służbowych, fałszowanie faktur sprzedażowych i zawyżanie cen, fikcyjne lub niepotrzebne zakupy, konflikty interesów i powiązania z dostawcami, niewłaściwe wykorzystywanie poufnych danych osobowych czy pracowniczych itd. Są to tylko niektóre przykłady najczęściej występujących nieprawidłowości i nadużyć. Wynikają one najczęściej z zewnętrznych

okoliczności i uwarunkowań, w jakich działa przedsiębiorca, a tym samym jego pracownicy, wewnętrznego zarządzania, ale także ze słabości lub różnie rozumianych potrzeb ludzi pracujących w danym przedsiębiorstwie.

Badania prowadzone w latach 70. XX w. na osobach skazanych za przestępstwa finansowe pozwoliły zdefiniować pewne stałe cechy każdego nadużycia. Opracowany przez Donalda Cressey'a trójkąt nadużyć⁴⁷ przedstawia mechanizm tego typu działań. U ich podstaw leży **presja** będąca głównym motywatorem podejmowania negatywnych czynności. Wynika ona z różnych motywacji – mogą to być wygórowane ambicje lub nierealne cele stawiane pracownikowi przez przełożonych, ale także potrzeby finansowe czy osobiste, takie jak chęć zakupu luksusowego domu czy wcześniejszej spłaty kredytu.

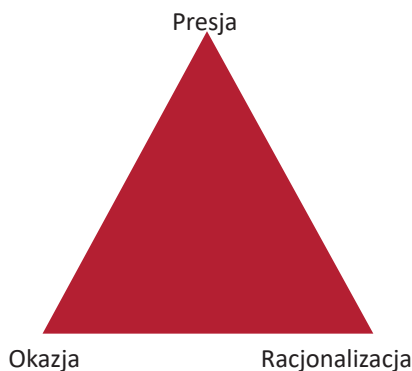
Silna motywacja powoduje, że pracownik zaczyna poszukiwać **okazji** do działania będącego źródłem powstania nadużycia. Może do tego wykorzystać niedoskonałą strukturę organizacyjną, niejasne podziały kompetencji i zakresy odpowiedzialności czy brak odpowiednio silnej kontroli procesów. Formą okazji mogą być również nieuczciwi współpracownicy w tzw. wrażliwych obszarach działania przedsiębiorstwa, np. w dziale zamówień publicznych czy w dziale sprzedaży.

Trzeci wierzchołek trójkąta nadużyć to **racjonalizacja**, która przejawia się w tym, że pracownik dopuszczający się nadużycia tłumaczy sam sobie, tj. usprawiedliwia swoje nieuczciwe postępowanie tym, że np. „to nie jest zabronione”, „przecież inni robią gorsze rzeczy” itp. Pozwala mu to zachować pozytywny obraz siebie i tym samym pozostać w przekonaniu,

⁴⁷ D. Cressey, *Other People's Money: A Study in the Social Psychology of Embezzlement*, Montclair, N.J.: Patterson Smith, 1973.

że to, co robi, jest postępowaniem całkowicie akceptowalnym i dopuszczalnym.

Dzięki teorii trójkąta nadużyć Cressey'a przedsiębiorca ma możliwość ustalenia, co należy zrobić, aby ograniczyć w swojej organizacji prawdopodobieństwo wystąpienia nadużyć; może zarówno zidentyfikować grupę pracowników szczególnego ryzyka (pracownicy żyjący ponad stan, mający kłopoty finansowe, cechujący się dużym przywiązaniem do kwestii materialnych), określić miejsca potencjalnego nadużycia, jak i opracować procesy oraz procedury, które utrudnią pracownikom racjonalizację zachowań szkodliwych dla firmy.



Jest rzeczą absolutnie oczywistą, że nadużycia występują w każdej organizacji, natomiast to, jak bardzo będą one rozpowszechnione, w dużej mierze zależy od poziomu akceptacji takich zachowań przez cały zespół pracowników, ale przede wszystkim przez kierownictwo i właścicieli. Jeśli nieetyczne postępowanie pracowników będą akceptowane i tolerowane przez innych pracowników, a w szczególności przez kadrę kierowniczą, wówczas staną się one normą, a nawet wzorcem zachowania. Ogromne znaczenie ma zatem postawa i zachowanie menadżerów średniego i wyższego szczebla – muszą oni dawać przykład oraz poprzez swoje

postępowanie, decyzje i sposób zarządzania w jasny sposób komunikować wszystkim podwładnym, jakie zachowania są standardem w ich organizacji. Więcej na ten temat można znaleźć w rozdziale 4 niniejszej publikacji.

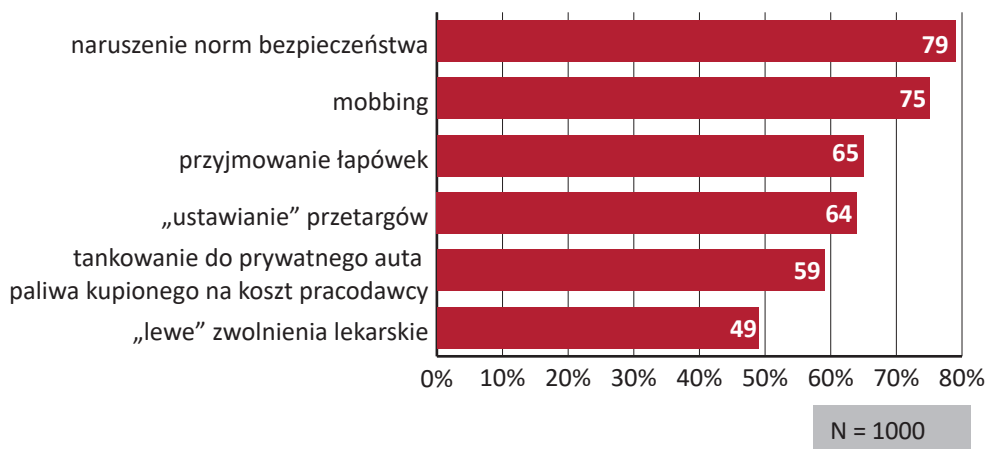
Wszystkie przypadki naruszeń, jeśli nie zostaną odpowiednio wcześniej wykryte i nie podejmie się w stosunku do nich właściwych działań naprawczych, mogą wywołać bardzo duże szkody dla organizacji. Zwykle pracownicy danej organizacji albo osoby z nią współpracujące w ramach swojej działalności zawodowej wiedzą, że w organizacji mają miejsce nieprawidłowości, znają ich mechanizmy i jako pierwsi mają możliwość odpowiedniego zareagowania. Osoby, które się na to zdecydują, są nazywane sygnalistami (ang. *whistleblowers*), a ich działalność jest definiowana jako *whistleblowing*, czyli zgłaszanie wewnątrz danej organizacji bądź właściwemu organowi na zewnątrz lub ujawnianie opinii publicznej informacji o nadużyciach w danej organizacji, które to informacje pozyskują w związku ze swoim zatrudnieniem lub współpracą z tą organizacją. Jest to termin powstały i powszechnie stosowany w anglosaskim kręgu kulturowym.

Jak wykazują badania to właśnie sygnaliści, funkcjonując wewnątrz danej organizacji, najlepiej wiedzą, kiedy i jakie problemy się w niej pojawiają, a taka swego rodzaju podpowieź płynąca z wewnętrznej struktury danego pracodawcy jest jednym z najskuteczniejszych narzędzi wykrywania nadużyć i nieprawidłowości w organizacji. Wiele z nadużyć nigdy nie zostałoby ujawnionych, gdyby nie zgłoszenia sygnalistów.

Niestety potencjalni sygnaliści niechętnie zgłaszają swoje podejrzenia z obawy przed odwetem i szykanami ze strony pracodawcy, kolegów z pracy i szerszego otoczenia. Boją się szykan, nie czują się dostatecznie bezpiecznie, aby ujawnić posiadane przez siebie informacje, co skutkuje mniejszą liczbą dokonywanych zgłoszeń nieprawidłowości, a tym samym –

niższym poziomem ich wykrywania i zwalczania. Ciche przyzwolenie i obawa przed byciem uznanym przez kolegów za donosiiciela nadal stanowią silną barierę przed zgłaszaniem nadużyć. Poparcie i zrozumienie celu zgłaszania nadużyć jest nadal na zbyt niskim poziomie – poniższy wykres przedstawia, jak kształtuje się poziom akceptacji działania sygnalistów w zależności od typu naruszeń⁴⁸.

Poparcie dla zgłaszania do przełożonego w zależności od typu nadużycia



Ponieważ jednak działalność sygnalistów nabiera coraz większego znaczenia dla procesu wykrywania nadużyć i egzekwowania stosowania przepisów prawa, objęcie ich skuteczną ochroną zapewniającą poczucie bezpieczeństwa, stało się bardzo ważnym celem ustawodawcy zarówno krajowego, jak i europejskiego. Duża część problemów i rozterek, na jakie napotykają sygnaliści – zarówno ci, którzy zdecydowali się zgłosić nadużycie, jak i ci, którzy tego nie zrobili – może bowiem zostać wyeliminowana lub znacznie ograniczona przez odpowiednie regulacje prawne,

⁴⁸ Raport z badania opinii publicznej Fundacji im. Stefana Batorego, *Gnębieni, podziwiani i ...zasługujący na ochronę. Polacy o sygnalistach*, G. Makowski, M. Waszak.

które zniwelują negatywne reperkusje grożące sygnalistom związane z dokonywanymi zgłoszeniami.

2. Ochrona sygnalistów wprowadzona na mocy Dyrektywy Parlamentu Europejskiego i Rady w sprawie ochrony osób zgłaszających przypadki naruszenia prawa Unii

16 kwietnia 2019 r. Parlament Europejski przyjął dyrektywę w sprawie ochrony osób zgłaszających przypadki naruszeń prawa Unii, czyli tzw. dyrektywę dotyczącą ochrony sygnalistów. Ma ona ułatwić egzekwowanie stosowania prawa Unii Europejskiej poprzez zagwarantowanie ochrony osobom zgłaszającym naruszenia tego prawa we wskazanych w dyrektywie obszarach.

Zgodnie z dyrektywą sygnalistą, któremu należy zapewnić ochronę, jest osoba już pracująca, która powzięła informacje o nieprawidłowości w związku ze swoją pracą, ale również osoba, której stosunek pracy zostanie dopiero nawiązany – wówczas zgłoszenie może dotyczyć nadużyć, o których osoba ta dowiedziała się na etapie rekrutacji. Zwykle nieprawidłowości takie dotyczą samego procesu rekrutacyjnego, np. nierównego traktowania, dyskryminacji czy naruszenia ochrony danych osobowych.

2.1. Status quo ochrony sygnalistów w UE

Komisja Europejska zwróciła uwagę na fakt, iż obecnie mechanizm ochrony sygnalistów jest w krajach Unii Europejskiej rozproszony i niejednolicie stosowany w odniesieniu do poszczególnych obszarów wspólnej polityki.

Ten brak spójności negatywnie wpływa na efektywność całego systemu Unii Europejskiej. Ponadto, jak podaje Komisja Europejska, straty spowodowane brakiem należytej ochrony sygnalistów na przykład przy zamówieniach publicznych wynoszą od 5,8 do nawet 9,6 miliardów euro w skali całej Unii Europejskiej.

Celem dyrektywy jest stworzenie kompleksowego systemu ochrony sygnalistów, który będzie obejmował wszystkie kraje członkowskie UE. Wyznacza ona jedynie minimalny standard ochrony, a zatem państwa członkowskie mają możliwość przyjęcia w swoim ustawodawstwie wyższego standardu.

2.2. Skutki dla przedsiębiorców

Dyrektywa przewiduje, że w każdej instytucji publicznej i prywatnej, zatrudniającej co najmniej 50 osób, będzie musiała zostać wprowadzona procedura zgłaszania nieprawidłowości czy nadużyć w miejscu pracy. Wymóg ten będzie dotyczyć również przedsiębiorców, których roczny obrót lub roczna suma bilansowa wynosi co najmniej 10 mln euro oraz tych, którzy działają w branży finansowej lub są narażeni na ryzyko związane z praniem pieniędzy lub finansowaniem terroryzmu.

Podmioty te będą musiały stworzyć wewnętrzne kanały przyjmowania zgłoszeń od sygnalistów, które zapewnią ochronę tożsamości osób zgłaszających. Co do zasady sygnaliści zdecydowanie łatwiej dokonywaliby zgłoszeń za pośrednictwem kanałów wewnętrznych działających u swojego pracodawcy. Dlatego też przedsiębiorcy powinni zachęcać sygnalistów do korzystania w pierwszej kolejności z wewnętrznych kanałów i zgłaszania naruszeń wewnątrz organizacji, szczególnie wtedy, gdy uznają, że naruszeniu można faktycznie skutecznie zaradzić w ramach organizacji i że nie ma ryzyka odwetu. Takie właśnie zgłoszenia

wewnętrzne są najefektywniejszym sposobem na poinformowanie o nieprawidłowościach konkretnych, właściwych osób w organizacji, które mogą przyczynić się do wczesnego i skutecznego wyeliminowania związanych z nimi zagrożeń.

Przedsiębiorcy będą musieli także przygotować procedury zgłaszania nieprawidłowości wewnątrz organizacji i poinformować o nich pracowników w sposób jasny i łatwo dostępny. Powinno się to przyczynić do promowania w organizacjach dobrej komunikacji i odpowiedzialności wszystkich pracowników za stosowanie przyjętych standardów postępowania. Oprócz wewnętrznych kanałów zgłaszania naruszeń przedsiębiorcy muszą poinformować o możliwości dokonywania zgłoszeń na zewnątrz organizacji do właściwych organów lub instytucji.

Po przyjęciu zgłoszenia od sygnalistów przedsiębiorcy będą mieli obowiązek podjąć działania następcze, zmierzające zarówno do wyjaśnienia sprawy i usunięcia negatywnych skutków naruszeń, jak i do podjęcia działań mających na celu zapewnienie sygnaliście ochrony. O planowanych lub podjętych działaniach następczych sygnalista powinien zostać poinformowany w rozsądnym terminie – w ciągu trzech miesięcy od zgłoszenia. Warto również takie działania uzasadnić, np. wyjaśnić, dlaczego zgłoszenie zostało przekazane do konkretnych komórek, innych kanałów lub uruchomiono konkretne procedury.

Należy pamiętać, aby osobę dokonującą zgłoszenia na bieżąco informować o postępach i wynikach wewnętrznego postępowania wyjaśniającego, tzn. o jego wszczęciu, zakończeniu (np. z braku wystarczających dowodów lub z innych powodów) czy przekazaniu do innych organów. Informując o ustaleniach poczynionych w jego toku, zawsze należy mieć na uwadze zarówno dobro toczącego się postępowania, jak i prawa osób, których zgłoszenie dotyczy.

Takie informowanie osoby dokonującej zgłoszenia o działaniach następczych podjętych w związku ze zgłoszeniem, ma kluczowe znaczenie dla budowania zaufania zarówno do obowiązujących w organizacji norm postępowania zgodnego z przepisami prawa, jak i do skuteczności samego systemu ochrony sygnalistów. Zmniejsza też ryzyko dokonywania przez pracowników ujawnień publicznych, grożących utratą reputacji organizacji.

Sygnaliści bowiem, oprócz zgłoszeń wewnętrznych i zewnętrznych, mogą dokonywać ujawnienia, czyli podania informacji o naruszeniu w miejscu pracy do publicznej wiadomości.

Procedura publiczna znajdzie zastosowanie wtedy, gdy:

- sygnalista najpierw dokonał zgłoszenia wewnętrznego lub zewnętrznego, lecz w odpowiedzi na jego zgłoszenie nie podjęto żadnych odpowiednich działań w terminie; lub
- nie można było od sygnalisty racjonalnie oczekiwać, że skorzysta z wewnętrznych lub zewnętrznych kanałów zgłaszania nieprawidłowości, z powodu bezpośredniego lub oczywistego zagrożenia dla interesu publicznego (np. zмова organu z podmiotem) ze względu na szczególne okoliczności sprawy (np. istnieje podejrzenie, że dowody zostaną ukryte) lub na ryzyko nieodwracalnej szkody (np. szkody dla integralności cielesnej).

Kolejnym obowiązkiem przedsiębiorcy związanym z systemem ochrony sygnalistów jest wyznaczenie osoby odpowiedzialnej za obsługiwanie kanałów zgłoszeń oraz za podejmowanie działań następczych – mogą to być osoby lub całe działy zarówno wewnątrz organizacji (np. dedykowana komórka lub powołany compliance officer), jak i osoby z zewnątrz (np. zewnętrzne firmy doradcze).

Jak już wspomniano, we wszystkich przypadkach zgłaszania naruszeń, zarówno za pomocą kanałów wewnętrznych, jak i zewnętrznych, sygnalista jest narażony na działania odwetowe ze strony pracodawcy bądź kolegów z pracy i dlatego dyrektywa nakłada na państwa członkowskie obowiązek podjęcia niezbędnych środków, aby zakazać wszelkich form takich działań.

2.3. Zakazane działania odwetowe

Dyrektywa mówi, że zabronione są w szczególności działania odwetowe polegające na:

- a) zawieszeniu, przymusowym urlopie bezpłatnym, zwolnieniu lub równoważnych środkach,
- b) degradacji lub wstrzymaniu awansu,
- c) przekazaniu obowiązków, zmianie miejsca pracy, obniżeniu wynagrodzenia, zmianie godzin pracy,
- d) wstrzymaniu szkoleń,
- e) negatywnej ocenie wyników lub negatywnej opinii o pracy,
- f) nałożeniu lub zastosowaniu jakiegokolwiek środka dyscyplinarnego, nagany lub innej kary, w tym finansowej,
- g) przymusie, zastraszaniu, mobbingu lub wykluczaniu,
- h) dyskryminacji, niekorzystnym lub niesprawiedliwym traktowaniu,
- i) nieprzekształceniu umowy o pracę na czas określony w umowę o pracę na czas nieokreślony, w sytuacji gdy pracownik mógł mieć uzasadnione oczekiwania, że zostanie mu zaoferowane stałe zatrudnienie,
- j) nieprzedłużeniu lub wcześniejszym rozwiązaniu umowy o pracę na czas określony,
- k) szkodzie, w tym nadszarpnięciu reputacji danej osoby, zwłaszcza w mediach społecznościowych, lub stracie finansowej, w tym stracie gospodarczej i utracie dochodu,
- l) umieszczeniu na czarnej liście na podstawie nieformalnego lub formalnego porozumienia sektorowego lub branżowego, co może

- skutkować tym, że dana osoba nie znajdzie w przyszłości zatrudnienia w danym sektorze lub danej branży,
- m) wcześniejszym rozwiązaniu lub wypowiedzeniu umowy dotyczącej towarów lub umowy o świadczenie usług,
 - n) odebraniu licencji lub zezwolenia,
 - o) skierowaniu na badania psychiatryczne lub lekarskie.

2.4. Przestanki objęcia sygnalisty ochroną

Bardzo istotnym aspektem w kontekście objęcia sygnalisty ochroną jest jego osobiste, subiektywne przekonanie o bezprawności czynu, który ma być zgłoszony. Aby móc bowiem skorzystać z ochrony, sygnalista musi mieć uzasadnione przekonanie, w świetle okoliczności i informacji jakimi dysponuje w momencie zgłaszania, że zgłaszane przez niego kwestie są prawdziwe. Taki wymóg stanowi z jednej strony zabezpieczenie przed zgłoszeniami dokonywanymi w złej wierze, niepoważnymi lub stanowiącymi nadużycie, a nawet przestępstwo, z drugiej zaś gwarantuje, że osoby, które w momencie zgłaszania celowo i świadomie przekazały błędne lub wprowadzające w błąd informacje, nie będą korzystały z ochrony.

Jeżeli sygnalista zgłosi informacje nieścisłe lub nieprawdziwe, jednak uczynił to na skutek niezamierzonego błędu, wówczas na mocy dyrektywy także będzie podlegał ochronie.

Niekiedy sygnalista ma podstawy przypuszczać, że zgłoszenie nieprawidłowości za pomocą kanałów wewnętrznych może negatywnie wpłynąć na skuteczność postępowania wyjaśniającego (np. z uwagi na udział osób mogących być bezpośrednio zaangażowanych w naruszenie) czy dochodzenia prowadzonego przez właściwe organy. Wówczas, dokonując zgłoszenia bezpośrednio za pomocą kanałów zewnętrznych

i z pominięciem kanałów wewnętrznych organizacji, także podlega ochronie.

Natomiast w przypadku kiedy sygnalista dokonuje ujawnienia informacji o nieprawidłowościach bezpośrednio do publicznej wiadomości (np. za pośrednictwem mediów), może podlegać ochronie tylko w przypadku, gdy mimo uprzedniego dokonania zgłoszenia wewnętrznego lub zewnętrznego, nadal nie zaradzono naruszeniu lub też, gdy sygnalista, z uwagi na szczególne okoliczności sprawy, która jest przedmiotem zgłoszenia, ma ważne powody, by sądzić, że naruszenie nie zostało właściwie ocenione lub zbadane lub nie podjęto żadnych odpowiednich działań zaradczych.

Zapewnienie skuteczności przepisów dotyczących ochrony sygnalistów, a także zachowanie wiarygodności całego systemu ochrony sygnalistów, wymaga wprowadzenia odpowiedniego systemu sankcji o charakterze karnym, cywilnym lub administracyjnym. Dyrektywa nakłada na państwa członkowskie obowiązek zapewnienia systemu kar zarówno dla przedsiębiorców, którzy dopuścili się działań odwetowych wobec sygnalistów, jak i dla samych sygnalistów, którzy świadomie, w złej wierze dokonali nieprawdziwego zgłoszenia lub ujawnienia *publicznego*.

Dyrektywa nie określa konkretnych sankcji, ale nakazuje, aby kary ustanowione przez poszczególne państwa członkowskie były skuteczne, proporcjonalne i odstraszające. Ich prewencyjny charakter ma zapobiegać podejmowaniu niedozwolonych działań odwetowych, jak również zniechęcić do dokonywania przez sygnalistów zgłoszeń w złej wierze.

2.5. Najważniejsze środki ochrony prawnej sygnalistów

Dyrektywa przewiduje również szereg środków prawnych chroniących sygnalistów. Sygnaliści zgłaszający nieprawidłowości do właściwych organów będą m.in. mieli zagwarantowaną anonimowość. Nadto państwa członkowskie mają obowiązek zapewnić im darmową i obszerną informację i porady na temat przysługujących im środków ochrony przed odwetem, a także skuteczną pomoc prawną w postępowaniu przed organem mającym mu zapewnić tę ochronę.

Bardzo ważne jest też to, że w wypadku wytoczenia przez sygnalistę uzasadnionego powództwa o odszkodowanie za szkodę, jaką poniósł na skutek skierowanych wobec niego działań odwetowych, ciężar udowodnienia, że szkoda nie powstała właśnie w związku z tymi działaniami odwetowymi, będzie spoczywał na pozwanym, czyli osobie, która dokonała odwetu (np. pracodawca). To ta osoba będzie musiała w procesie udowodnić, że nie podejmowała zabronionych działań odwetowych.

Dyrektywa o ochronie sygnalistów wprowadza zasady wchodzące w zakres systemu compliance, którego znaczenie w obrocie gospodarczym ciągle wzrasta. Dla wielu przedsiębiorców dostosowanie się do standardów stawianych przez dyrektywę może być dużym wyzwaniem, a mają na to czas do 15 maja 2021 r.

3. Sygnalista na gruncie prawa polskiego

W Polsce pojawiają się kolejne projekty ustaw, które w pewnym zakresie regulują kwestie związane z ochroną sygnalistów, brak jest jednak aktu prawnego, który w kompleksowy sposób uregulowałby tę problematykę

i to w odniesieniu do wszystkich przedsiębiorców, niezależnie od wielkości, przedmiotu działalności itd.

3.1. *Whistleblowing* w ustawie AML

Obowiązek zapewnienia sygnalistom możliwości zgłaszania nieprawidłowości wprowadza ustawa z dnia 13 lipca 2018 r. o przeciwdziałaniu praniu pieniędzy i finansowaniu terroryzmu (dalej: ustawa AML). Ustawa reguluje zgłaszanie nieprawidłowości, ale tylko w zakresie prania pieniędzy oraz finansowania terroryzmu. Nakłada na przedsiębiorców obowiązek opracowania i wdrożenia procedury anonimowego zgłaszania rzeczywistych i potencjalnych naruszeń wyłącznie w tym zakresie. Obowiązek ten dotyczy tylko tych przedsiębiorców, którzy prowadzą działalność, przy wykonywaniu której występuje zwiększone ryzyko wystąpienia transakcji prania pieniędzy lub finansowania terroryzmu, np. instytucje finansowe, domy maklerskie, biura rachunkowe, doradcy podatkowi lub prawnicy, którzy są tzw. instytucjami obowiązanyymi w rozumieniu wskazanej ustawy.

Podstawowe założenia procedury systemu anonimowego zgłaszania naruszeń wprowadzonej niniejszą ustawą obejmują następujące kwestie:

- zgłoszenia dokonywane przez sygnalistów dotyczą rzeczywistych lub potencjalnych naruszeń przepisów z zakresu przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu; mogą być dokonywane przez pracowników lub inne osoby wykonujące czynności na rzecz instytucji obowiązanej, np. na podstawie umów cywilnoprawnych, B2B, przez pracowników podwykonawców czy pośredników;
- procedura powinna określać osobę odpowiedzialną za odbieranie zgłoszeń w instytucji obowiązanej oraz sposób ich odbierania;

- procedura powinna awierać informację odnośnie rodzaju i charakteru działań następczych podejmowanych przez instytucję obowiązującą po odebraniu zgłoszenia.

Procedura winna także określać sposób ochrony danych osobowych pracownika dokonującego zgłoszenia oraz osoby, której zarzuca się dokonanie naruszenia, zgodnie z przepisami o ochronie danych osobowych oraz zasady zachowania poufności w przypadku ujawnienia tożsamości tych osób.

Ustawa istotnie wzmacnia rolę sygnalisty w procesie wykrywania naruszeń i nieprawidłowości – zawiera wytyczne dla instytucji obowiązanych dotyczące obowiązku zapewnienia ochrony pracownikom dokonującym zgłoszenia, przy czym minimalny poziom tej ochrony obejmuje zapobieganie działaniom o charakterze represyjnym, dyskryminacyjnym lub innym rodzajom niesprawiedliwego traktowania. Jej słabością jest jednak to, że nie obejmuje ona wszystkich podmiotów, a jedynie te, które wypełniają definicję podmiotów obowiązanych.

3.2. Projekt ustawy o jawności życia publicznego

Nieco inne spojrzenie na sygnalistę i jego ochronę prawną zawierał projekt ustawy o jawności życia publicznego.

Status sygnalisty byłby nadawany przez prokuratora osobom współpracującym z organami ścigania i zgłaszającym możliwość popełnienia przestępstwa wymienionego w art. 81 ust. 1 projektu (m.in. przestępstwo łapownictwa, przekroczenia uprawnień przez funkcjonariusza publicznego, udział w zorganizowanej grupie przestępczej, nadużycie zaufania itd.), jeśli ten fakt mógłby niekorzystnie wpłynąć na ich sytuację życiową, zawodową lub materialną. Informacje przekazane przez sygnalistę musiałyby być wiarygodne, a on sam formalnie musiałby złożyć zeznania.

W rozumieniu projektu status sygnalisty mógłby przysługiwać nie tylko osobie zatrudnionej na podstawie stosunku pracy, ale także na podstawie umowy cywilnoprawnej. Takiej osobie pracodawca nie mógłby bez zgody prokuratora wypowiedzieć umowy o pracę ani jednostronnie zmienić jej warunków na mniej korzystne, zwłaszcza w zakresie miejsca pracy, czasu wykonywania pracy lub warunków wynagradzania. Zgoda prokuratora nie byłaby wymagana w przypadku porozumienia stron albo zmiany warunków umowy na korzystniejsze dla sygnalisty.

Okres ochronny sygnalisty trwałby od momentu nadania mu tego statusu i kończyłby się z chwilą umorzenia postępowania lub zakończenia prawomocnym orzeczeniem postępowania karnego. W praktyce mogło to zatem oznaczać wieloletnią ochronę przed wypowiedzeniem.

W projekcie posłużono się co prawda pojęciem sygnalisty, jednak definicja prawna, a także środki ochrony prawnej osób zgłaszających nadużycia w miejscu pracy w żadnym razie nie odzwierciedlają idei *whistleblowingu* i standardów formułowanych przez Radę Europu i ONZ⁴⁹.

Prace nad tym projektem trwają od października 2017 r. i w chwili oddawania niniejszej publikacji do składu nie była znana ostateczna wersja projektu tego aktu prawnego.

3.3. Projekt ustawy o odpowiedzialności podmiotów zbiorowych za czyny zabronione pod groźbą kary

Szerszy zakres regulacji dotyczącej sygnalistów i ich ochrony prawnej mają zapisy projektu ustawy o odpowiedzialności podmiotów zbiorowych za czyny zabronione pod groźbą kary.

⁴⁹ *Ibidem*.

Projektowane przepisy mają przede wszystkim rozszerzyć podstawę odpowiedzialności podmiotów zbiorowych za czyny zabronione. Ustawodawca wprowadza definicję podmiotu zbiorowego, z której wynika, że również i tym razem nie wszystkie podmioty miałyby być objęte dyspozycją tej ustawy, aczkolwiek zakres ten jest niewątpliwie szerszy niż w ustawie AML. Regulacje zawarte w projekcie ustawy nie będą jednak dotyczyć pracowników zatrudnionych przez jednoosobowych przedsiębiorców.

W myśl projektu sygnalistą, któremu mają przysługiwać uprawnienia ochronne, jest nie tylko pracownik podmiotu zbiorowego, niezależnie od tego, czy jest on zatrudniony na czas określony, czy nieokreślony, ale także członek jego organu lub inne osoby, które na podstawie czynności prawnej działają w imieniu lub w interesie podmiotu zbiorowego. Mogą to zatem być również pełnomocnicy, podwykonawcy, stażyści czy praktykanci.

Projekt ustawy reguluje odpowiedzialność podmiotu zbiorowego za działania wobec takich osób zgłaszających nieprawidłowości – organy podmiotu zbiorowego (zarząd czy rada nadzorcza) lub osoby sprawujące wewnętrzny nadzór nad przestrzeganiem przez podmiot zasad i regulacji dotyczących jego działalności, mają obowiązek podjąć wszelkie czynności mające na celu wyjaśnienie informacji zgłaszanych przez sygnalistów. Chodzi o informacje świadczące o:

- podejrzeniu przygotowania, usiłowania lub popełnienia czynu zabronionego;
- niedopełnieniu obowiązków lub nadużyciu uprawnień przez organy podmiotu zbiorowego lub inne – wymienione w ustawie osoby – działające w jego imieniu, na jego rzecz lub zlecenie (krąg osób, za których działanie podmiot może ponosić odpowiedzialność jest tak szeroki, że faktycznie uzasadnia konieczność wprowadzenia w podmiocie zbiorowym skutecznego systemu zarządzania ryzykiem);

- niezachowaniu przez powyższe osoby należytej staranności, wymaganej w danych okolicznościach; lub
- nieprawidłowościach w organizacji działalności podmiotu zbiorowego, które mogłyby prowadzić do popełnienia czynu zabronionego.

Zgłoszenia mogą dotyczyć zarówno faktycznych i rzeczywistych zdarzeń, jak i zdarzeń przyszłych, np. planowania przez członka zarządu wyprowadzenia środków finansowych ze spółki.

Ponieważ nieodzownym elementem skutecznego funkcjonowania systemu zgłaszania nieprawidłowości jest zapewnienie ochrony prawnej osób dokonujących zgłoszenia, projekt zakłada istotne zwiększenie bezpieczeństwa prawnego sygnalistów. Jest to tym bardziej konieczne, że obecne uregulowania w tym zakresie, znajdujące się głównie w kodeksie pracy, nie gwarantują sygnalistom kompleksowej i wystarczającej ochrony prawnej przed represjami i działaniami odwetowymi mogącymi ich spotkać w miejscu pracy w związku z faktem dokonania zgłoszenia. Jako najbardziej dotkliwe zagrożenie dla sygnalisty projekt wskazał utratę pracy, ale może to być także brak dostępu do szkoleń czy pozbawienie możliwości awansu.

Na wypadek zastosowania wobec sygnalisty tego typu represji, o ile informacje przez niego zgłoszone były zasadne i mogły doprowadzić do zapobiegnięcia lub szybszego wykrycia czynu zabronionego, sąd może orzec przywrócenie takiej osoby do pracy lub zasądzić odszkodowanie – zgodnie z przepisami kodeksu pracy. Nowością jest natomiast wprowadzenie możliwości orzeczenia przez sąd odszkodowania za cały okres pozostawania bez pracy. W przypadku długotrwałego procesu wysokość odszkodowania może stanowić nawet równowartość kilkunastu lub więcej miesięcznych wynagrodzeń.

Przywrócenie do pracy i odszkodowanie co do zasady nie będzie przysługiwać osobie, która była sprawcą zabronionego czynu, chyba że osoba ta ujawniła podmiotowi zbiorowemu i organom ścigania wszystkie istotne okoliczności popełnienia czynu.

Ponieważ ustawa miałyby wprowadzić obowiązek dla podmiotu zbiorowego przeprowadzenia postępowania wyjaśniającego w każdym przypadku zgłoszenia przez sygnalistę naruszenia mogącego rodzić odpowiedzialność tego podmiotu za czyn zabroniony, dla podmiotów zbiorowych jest rekomendowane wdrożenie odpowiednich procedur, które zapewniłyby sygnalistom możliwość bezpiecznego zgłaszania wszelkich ewentualnych nadużyć. Procedury takie powinny wyraźnie określać zasady postępowania przy dokonywaniu zgłoszenia, tzn. jak (przy użyciu jakich narzędzi), kiedy i komu należy dokonać zgłoszenia, a także jaki jest tryb przyjmowania i dalszego procedowania zgłoszonych naruszeń. Ustawa co prawda nie nakłada na przedsiębiorców wprost obowiązku stworzenia takiej procedury zgłaszania nieprawidłowości i ochrony sygnalistów, jednakże nie wydaje się możliwe zarządzanie takimi zgłoszeniami przez powołane do tego osoby bez konkretnych wytycznych ujętych w ramach proceduralnych. Przygotowanie i skuteczne wdrożenie mechanizmów *whistleblowingu* jest też przejawem zachowania należytej staranności przez osoby odpowiedzialne w spółce za przestrzeganie norm i przepisów prawa.

Podmiot, który nie usunie stwierdzonych w postępowaniu wyjaśniającym nieprawidłowości, musi liczyć się z ryzykiem nałożenia na niego kary w podwójnej wysokości, czyli do 60 mln zł.

Projekt tej ustawy jest najbardziej zaawansowany w procesie legislacyjnym, tzn. w styczniu 2019 r. został skierowany do konsultacji, jednak w chwili oddawania niniejszej publikacji do składu nie była znana ostateczna wersja projektu tego aktu prawnego.

4. Ochrona sygnalistów w Polsce – *de lege ferenda*

Mimo iż tematyka compliance od kilku lat zyskuje na znaczeniu, a świadomość przedsiębiorców w tym zakresie powoli rośnie, sygnalizowanie nadużyć nadal nie jest popularne w naszej kulturze i często postrzegane jest jako naganne donosicielstwo, które należy piętnować i eliminować. Jednakże, jak wynika z badań przeprowadzonych w roku 2018 przez Association of Certified Fraud Examiners (ACFE), to właśnie sygnaliści są głównym źródłem wykrywania wszelkich nieprawidłowości w sektorze prywatnym, a zatem ich rola w walce z nieprawidłowościami, skutkującymi odpowiedzialnością przedsiębiorców, nie może zostać niedoceniona, a ich pozycja musi być odpowiednio chroniona.

System informowania o nieprawidłowościach (SIN), będący narzędziem systemu zarządzania ryzykiem w przedsiębiorstwie, tylko wtedy jest skuteczny, kiedy zapewnia sygnalistom pełną ochronę i bezpieczeństwo. Mechanizm zgłaszania nieprawidłowości musi opierać się na założeniu, że każdy pracownik ma możliwość przekazania informacji o zauważonych nieprawidłowościach za pośrednictwem specjalnego kanału informacji, który jednak gwarantuje zachowanie anonimowości i zapewnia skuteczną ochronę prawną. Takim kanałem może być specjalna skrzynka mailingowa czy dedykowany program informatyczny. Ważne jest, aby sygnalista wiedział, że jego informacja nie trafi w przysłowiową próżnię, tzn. wiedział jakie działania wyjaśniające i naprawcze zostaną podjęte przez pracodawcę (organizację) po dokonaniu zgłoszenia i przede wszystkim – aby czuł się bezpiecznie i wiedział, że nie grozi mu za to prześladowanie, ostracyzm ze strony współpracowników, często prowadzący do mobbingu, utrata pracy czy też inne negatywne konsekwencje. Obawa przed tymi właśnie

konsekwencjami skutkuje tym, że wiele nieprawidłowości i zagrożeń nie jest zgłaszanych przez potencjalnych sygnalistów.

Niestety obecnie (oprócz ograniczonej podmiotowo ochrony przewidzianej w ustawie AML) jedynym gwarantem bezpieczeństwa sygnalisty jest jego anonimowość. Nie jest to ochrona wystarczająca, chociażby z tego względu, że na skutek zgłoszonych nieprawidłowości mogłoby dojść do postępowania sądowego i konieczności ujawnienia się sygnalisty.

Dlatego też do czasu implementacji przez Polskę dyrektywy o ochronie sygnalistów, przedsiębiorca, który chce efektywnie zarządzać ryzykiem, sam musi zadbać o stworzenie procedury *whistleblowing*, która zagwarantuje sygnalistom skuteczną ochronę prawną przed działaniami odwetowymi i represyjnymi. Zagwarantowanie tej ochrony pozwoli zbudować zaufanie potencjalnych sygnalistów do systemu zgłaszania nieprawidłowości i wzmocnić ich odpowiedzialność za przedsiębiorstwo.

Zgłoszenie nieprawidłowości dokonane przez pracownika na poziomie samej organizacji, czyli kanałami wewnętrznymi, daje szansę na rzetelne sprawdzenie tego zgłoszenia jeszcze na wczesnym etapie, zbadanie przyczyn i szybkie podjęcie działań naprawczych. Pozwala to niejednokrotnie na uniknięcie ujawnienia informacji na zewnątrz organizacji, co oznacza, że nie trafi ona do opinii publicznej i nie wywoła skandalu, którego skutkiem najczęściej są nie tylko ogromne straty finansowe, ale przede wszystkim najbardziej dotkliwa utrata budowanej przez lata renomy przedsiębiorcy. Nie trzeba chyba w tym miejscu wspominać, że koszty tego zwykle przewyższają trud związany z wprowadzeniem skutecznego systemu informowania o nieprawidłowościach.

Rozdział 4. Rola kadry menadżerskiej

Barbara Kaczała

1. Etyka i zgodność z prawem w przedsiębiorstwie – motywacja do „gry fair play”

Dynamika obecnego otoczenia gospodarczego, zwiększona aktywność organów dochodzeniowych oraz surowe wymogi prawne przyczyniły się do tego, że pojęcie compliance zaczęło zyskiwać na znaczeniu nie tylko w szeroko rozumianym sektorze finansowym, ale również wśród małych i średnich przedsiębiorców (MŚP).

W pierwszym przypadku sprecyzowane wymogi regulacyjne dotyczące zapewnienia wewnętrznych mechanizmów zgodności funkcjonują od dawna, jednak dla wielu małych i średnich prywatnych firm tematyka ta jest nowa. Wdrażanie systemu compliance nie jest natomiast obce podmiotom z kapitałem zagranicznym, którym spółki-matki niejednokrotnie narzucają konieczność przyjęcia np. kodeksu etycznego koncernu, a także stosowanie jednolitych rozwiązań przyjętych na poziomie grupy (np. powołanie compliance officer'a). Nie jest to równoznaczne ze skutecznością systemu compliance. Samo formalne zaaprobowanie określonych rozwiązań bez uwzględnienia kontekstu krajowego nie

gwarantuje bowiem sukcesu. Stanowi jednak punkt wyjścia do rozważań nad ryzykami występującymi w danej organizacji, co w założeniu ma doprowadzić do stworzenia systemu spójnego, dostosowanego do konkretnej firmy. Tymczasem wielu polskich przedsiębiorców podchodzi do tej tematyki ostrożnie, traktując compliance nie jako szansę na ochronę przed niekorzystnymi zjawiskami (np. korupcją, mobbingiem, nadużyciami), a jako dodatkową konieczną do spełnienia formalność. Takie podejście jest niezrozumiałe, ponieważ nie uwzględnia korzyści, które w dłuższej perspektywie czasowej przynosi system zarządzania zgodnością. „Abstrahując od licznych korzyści jakościowych, jakie wynikają dla przedsiębiorstwa z wprowadzenia sprawnego systemu zarządzania compliance, traktowany powinien być on jako inwestycja dająca szybko wysoką stopę zwrotu: system compliance nie tylko wpływa na polepszenie ratingu przedsiębiorstwa, obniża koszty doradztwa prawnego i stawek ubezpieczeniowych dla kadry zarządzającej, ale może również w istotny sposób przyczynić się do sukcesu przedsiębiorstwa”⁵⁰.

Biorąc to pod uwagę, należy zauważyć, że wprowadzenie sprawnego systemu compliance powinno stanowić dzisiaj standard będący wyrazem poszanowania zasad moralnych i etycznych w biznesie, a także spójnej wizji solidnej i uczciwej organizacji. Niezależnie od otoczenia prawnego te elementy są brane pod uwagę coraz częściej w codziennym życiu biznesowym, tzn. w praktyce zawierania umów, weryfikowaniu kontrahentów, certyfikacji (np. IATF w branży motoryzacyjnej). W tym kontekście jest istotne to, w jaki sposób przedsiębiorca zdefiniuje zasady etyczne, którymi kieruje się w swojej działalności. To one bowiem będą wyznaczały motywację do tego, aby rozpocząć proces wdrażania systemu zgodności (CMS). Można spotkać się z podziałem na wartości dotyczące

⁵⁰ Prof. B. Makowicz, *Metody efektywnego kształtowania systemów „compliance” – Wprowadzenie*, [w:] *Monitor Prawniczy* 2013, Nr 23

stricte sfery biznesowej – np. jakość obsługi, podejście do kontrahenta, sposób realizowania wyników finansowych – oraz sfery etycznej rozumianej jako wykazywanie takich zasad, jak lojalność, szacunek czy uczciwość⁵¹.

Motywacja do budowania systemu compliance nie powinna zatem wynikać jedynie z chęci uniknięcia czy ograniczenia odpowiedzialności. Jako przykład takiej motywacji można wskazać na przedsiębiorców, którzy są tzw. „instytucjami obowiązanyymi” w rozumieniu przepisów ustawy o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu. Warto zauważyć, że ten akt prawny rozszerzył znacząco grono podmiotów, które muszą stosować tzw. środki bezpieczeństwa finansowego. Tym samym podmioty prowadzące na przykład działalność w zakresie usługowego prowadzenia ksiąg rachunkowych czy też przedsiębiorcy świadczący usługi polegające na zapewnianiu siedziby, adresu prowadzenia działalności lub adresu korespondencyjnego oraz innych pokrewnych usług osobie prawnej lub jednostce organizacyjnej nieposiadającej osobowości prawnej, są zmuszone do zetknięcia się z surowymi wymogami ww. ustawy. Ich obowiązkiem jest na przykład wprowadzenie procedury wewnętrznej zawierającej m.in. zasady zgłaszania przez pracowników rzeczywistych lub potencjalnych naruszeń przepisów z zakresu przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu. Niedostosowanie się do tych wymogów jest zagrożone możliwością nałożenia wysokiej kary finansowej. W obliczu dotkliwych sankcji, wśród wielu przedsiębiorców z sektora prywatnego objętych wspomnianymi przepisami, a którzy po raz pierwszy stykają się z tematyką compliance, może dojść do wystąpienia niekorzystnej struktury motywacyjnej polegającej na podejściu formalnym zamiast efektywnym. A trzeba pamiętać, że miarą skuteczności systemu compliance

⁵¹ Raport Instytutu Institute of Business Ethics, *Corporate Ethics Policies and Programmes. 2016 UK and Continental Europe Survey*, 2016 r.

nie jest liczba procedur obowiązujących w firmie, lecz ich faktyczne obowiązywanie i stosowanie.



Warto pamiętać o tym, że wdrożenie skutecznego systemu compliance powinno opierać się na zasadzie ryzyka (ang. *risk based approach*) oraz że nie powinno być budowane w pośpiechu. Jest to proces, do którego należy podejść cierpliwie, dlatego że jego podstawą jest zbudowanie odpowiedniej kultury organizacji, a ta z kolei wiąże się niejednokrotnie z barierami w budowaniu postaw prospołecznych. O ile zatem pierwszy impuls do budowania compliance w organizacji powinien zawsze pojawiać się na szczeblu kadry zarządzającej – czyli w myśl zasady *Tone from the Top* – o tyle skuteczność systemu będzie zależna już także od mentalności społecznej. Jeśli te dwie składowe – tzn. moralność oraz obowiązujące normy wewnętrzne i zewnętrzne – będą szły ze sobą w parze, można mówić o spójności systemu. W przeciwnym razie compliance będzie jedynie wyrazem ruchów pozorowanych⁵².

⁵² Dr W. Banach, *Kulturowe bariery w kształtowaniu postaw prospołecznych wśród uczestników życia gospodarczego w Polsce*, [w:] *Ruch Prawniczy, Ekonomiczny i Socjologiczny* 2017, Nr 4

2. Rola kadry zarządzającej – odpowiedzialność i mechanizmy jej ograniczenia

Kluczowe dla zrozumienia istoty compliance jest uświadomienie sobie, że nie istnieje jedyny słuszny model tego systemu. Oznacza to, że powinien on być zawsze osadzony w strukturach i realiach konkretnej organizacji. Bardzo ważną rolę pełni w tym procesie kadra zarządzająca. To jej zadaniem jest promowanie odpowiedniej kultury korporacyjnej i stosowanie zasad compliance⁵³.

2.1. Definicja kadry zarządzającej

Kadra zarządzająca nie ma swojej definicji legalnej. Pojęcie to często jest używane zamiennie z określeniami kadra kierownicza oraz kadra menadżerska. Chodzi tu o te osoby, które skupiają kompetencje decyzyjne w danej organizacji. W zależności od formy prawnej mogą się różnić nazewnictwem. Przykładowo w spółce z ograniczoną odpowiedzialnością będzie to zarząd, któremu przysługuje domniemanie kompetencji i który reprezentuje spółkę oraz prowadzi jej sprawy. Jako kadrę zarządzającą będziemy jednak rozumieli także np. prokurentów czy dyrektorów poszczególnych działów – w zależności od tego, jakie kompetencje decyzyjne są im przyznane.

W przepisach powszechnie obowiązujących zamiennie przeplatają się wyżej wskazane określenia. Na przykład w art. 296a kodeksu karnego,

⁵³ M. B. Borowa, *Program „compliance” – przepis na sukces. Jakie wymagania powinny być spełnione z praktycznego punktu widzenia?*, [w:] *Monitor Prawniczy* 2013, Nr 23

który penalizuje tzw. korupcję menadżerską, jest mowa o osobie „pełniącej funkcję kierowniczą w jednostce organizacyjnej wykonującej działalność gospodarczą”⁵⁴.

Z kolei ustawa o rachunkowości w swojej systematyce definicyjnej posługuje się pojęciem „kierownika jednostki”, przez którego rozumie się:

- członka zarządu lub innego organu zarządzającego, a jeżeli organ jest wieloosobowy – członków tego organu, z wyłączeniem pełnomocników ustanowionych przez jednostkę;
- w przypadku spółki jawnej i spółki cywilnej za kierownika jednostki uważa się wspólników prowadzących sprawę spółki;
- w przypadku spółki partnerskiej – wspólników prowadzących sprawę spółki albo zarząd;
- w odniesieniu do spółki komandytowej i spółki komandytowo-akcyjnej – komplementariuszy prowadzących sprawę spółki;
- w przypadku osoby fizycznej prowadzącej działalność gospodarczą za kierownika jednostki uważa się tę osobę.

Co do zasady nie istnieje katalog zamknięty pojęcia kadry zarządzającej i określenie, kto do niej należy, powinno być dokonywane w zależności od konkretnego przypadku. „Pełnienie funkcji kierowniczej należy ustalać na podstawie struktury organizacyjnej [...] jednostki z uwzględnieniem

⁵⁴ Art. 296a § 1 kodeksu karnego: Kto, pełniąc funkcję kierowniczą w jednostce organizacyjnej wykonującej działalność gospodarczą lub pozostając z nią w stosunku pracy, umowy zlecenia lub umowy o dzieło, żąda lub przyjmuje korzyść majątkową lub osobistą albo jej obietnicę, w zamian za nadużycie udzielonych mu uprawnień lub niedopełnienie ciążącego na nim obowiązku mogące wyrządzić tej jednostce szkodę majątkową albo stanowiące czyn nieuczciwej konkurencji lub niedopuszczalną czynność preferencyjną na rzecz nabywcy lub odbiorcy towaru, usługi lub świadczenia, podlega karze pozbawienia wolności od 3 miesięcy do lat 5.

zakresu kompetencji sprawcy, które powinny mieć charakter władczy, związany z podejmowaniem decyzji”⁵⁵.

2.2. Odpowiedzialność członków zarządu

Wiele regulacji odnosi się jednak wprost do członków zarządu, zawężając jednocześnie zakres podmiotowy stosowania określonych przepisów. Forma prawna prowadzonej działalności determinuje tenże zakres odpowiedzialności oraz jej podstawy. Na przykład osoba fizyczna prowadząca jednoosobową działalność gospodarczą jest odpowiedzialna za zobowiązania zaciągnięte w ramach swojej działalności całym majątkiem osobistym i bez ograniczeń. Nie ma tutaj rozróżnienia na majątek przedsiębiorstwa i na majątek osobisty. Jest to najprostsza forma prowadzenia działalności, ale jednocześnie zakłada bardzo szeroką odpowiedzialność.

W przypadku spółek kapitałowych (spółka z o.o. oraz spółka akcyjnych) ma zastosowanie tzw. teoria organów. Spółka oraz jej organy to niejako odrębne byty. W tym kontekście również sama spółka posiada własny majątek, który nie jest jednocześnie majątkiem członków zarządu. Należy jednak zauważyć, że ich odpowiedzialność osobista jest bardzo szeroka i kształtuje się w różnych obszarach.

To właśnie szeroki wymiar odpowiedzialności – począwszy od surowej odpowiedzialności karnoskarbowej, poprzez odpowiedzialność cywilnoprawną i administracyjną, a skończywszy na wewnątrzorganizacyjnej – powoduje, że członkowie zarządu w istocie powinni regularnie dysponować możliwie szeroką wiedzą na temat aktualnych spraw spółki. Sytuacja taka może być trudna do osiągnięcia; często niezbędne jest

⁵⁵ Prof. K. Wiak, *Kodeks karny. Komentarz*, pod red. prof. Alicji Grześkowiak, Warszawa 2019

bowiem cedowanie określonych obowiązków na współpracowników. Budowa efektywnego systemu compliance rozumianego jako system naczyń połączonych – w tym np. przestrzeganie zasady czterech oczu, czyli kontroli przez dwie niezależne osoby – stanowi nieodzowny element, który może pozwolić członkom zarządu uchronić się przed sytuacją wystąpienia nieprawidłowości, w tym naruszenia prawa.

Przykład

Członek zarządu PRACOWITY PIOTR działający w imieniu spółki SUPER SPÓŁKA (spółka z o.o.) i pełniący w niej jednocześnie funkcję dyrektora handlowego prowadzi negocjacje z członkami zarządu kontrahenta KANCIARZ co do umowy na dostawę produktów. PRACOWITY PIOTR nie jest jedynym członkiem zarządu. Oprócz niego funkcję tę pełni również AMBITNY ANDRZEJ.

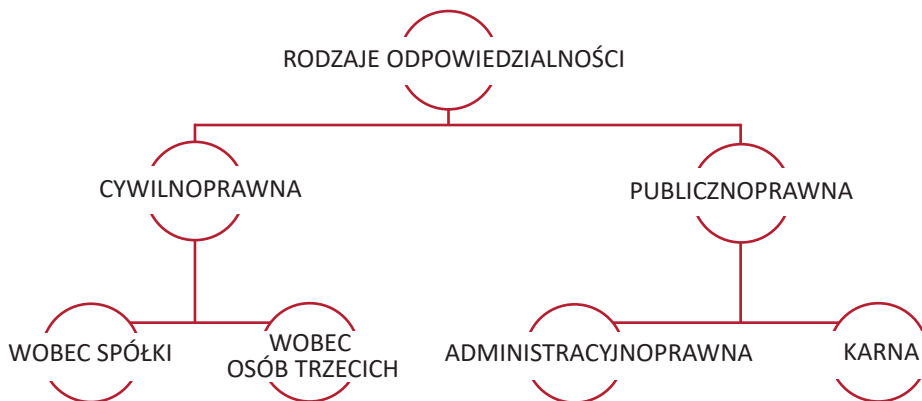
Każdy z członków zarządu jest uprawniony do jednoosobowej reprezentacji spółki. Nie istnieją żadne wewnętrzne procedury regulujące podział kompetencji ani sposób weryfikacji kontrahentów. W ramach swojej bieżącej działalności obaj członkowie zarządu mają przysłowiową wolną rękę co do wyboru dostawców i negocjowania z nimi umów. PRACOWITY PIOTR zawiera niekorzystną umowę z dostawcą. Oferuje on wprawdzie najatrakcyjniejsze warunki cenowe na dostawę półproduktów, jednak nie posiada wymaganych prawem certyfikatów jakościowych. Wkrótce okazuje się, że półprodukty są wadliwe.

Dostawca nie spełnia obowiązków gwarancyjnych. Klienci SUPER SPÓŁKI zaczynają występować z roszczeniami o naprawę. Sama spółka nie jest w stanie wywiązywać się ze swoich zobowiązań. Musi zlecać naprawy na zewnątrz, aby zachować klientów. Popada w tarapaty finansowe. Wkrótce jest zmuszona złożyć wniosek o ogłoszenie upadłości.

Konsekwencje

Po pierwsze należy podkreślić, że członek zarządu nie zachował należytej staranności w działaniu. Nie zostały zastosowane żadne wewnętrzne mechanizmy weryfikacji kontrahenta np. pod kątem jego sytuacji finansowej. Takie działanie ostatecznie doprowadziło do niewypłacalności spółki. Warto zauważyć, że w przypadku niewywiązywania się przez spółkę z płatności na rzecz kontrahentów, możliwa jest ewentualna osobista odpowiedzialność członków zarządu za jej zobowiązania. Co prawda od odpowiedzialności tej można się uwolnić, jednak jej reżim jest surowy, a ciężar dowodzenia w tym zakresie obciąża członka zarządu.

Niewątpliwie zatem duży wpływ na motywację kadry zarządzającej będzie miała kwestia własnej odpowiedzialności. Wdrożenie skutecznego systemu compliance ściśle się z nią wiąże, ponieważ pozwala na przykład na szybkie wykrycie nieprawidłowości, podjęcie zawczasu odpowiednich działań naprawczych, co w konsekwencji może ochronić członka zarządu od naruszenia prawa i poniesienia dotkliwych konsekwencji.



Można wyróżnić szereg możliwych reżimów odpowiedzialności.

Po pierwsze odpowiedzialność cywilnoprawna, czyli inaczej mówiąc – prywatnoprawna, w tym:

- wobec spółki (np. za szkodę wyrządzoną w szczególności zawinionym działaniem lub zaniechaniem sprzecznym z prawem lub postanowieniami umowy; przy tworzeniu spółki; poprzez naruszenie zakazu konkurencji);
- wobec osób trzecich (przede wszystkim za zobowiązania spółki) – tzw. odpowiedzialność na zewnątrz, w stosunku do wierzycieli, kontrahentów, dostawców.

Po drugie członek zarządu odpowiada także na gruncie przepisów o charakterze publicznoprawnym.

Wyróżnić można tutaj odpowiedzialność:

- administracyjnoprawną,
- karną, w tym karnoskarbową.

Nie jest możliwe enumeratywne wyliczenie w tym miejscu wszystkich podstaw potencjalnej odpowiedzialności. Członkowie zarządu odpowiadają na przykład na gruncie przepisów kodeksu spółek handlowych przede wszystkim za zawyżenie wartości aportu, za naruszenie zakazu konkurencji, ale również za dokonanie niezgodnej z prawem lub umową spółki wypłaty na rzecz wspólnika. Dodatkowo członek zarządu może odpowiadać nie tylko za niezgodne z prawem działania swoich pracowników, ale także kontrahentów.

Ponadto jeżeli egzekucja przeciwko spółce okaże się bezskuteczna, członkowie zarządu odpowiadają solidarnie za jej zobowiązania całym swoim majątkiem osobistym (art. 299 kodeksu spółek handlowych). Jest to tzw. odpowiedzialność wobec osób trzecich i jest ona bardzo surowa. To na członku zarządu spoczywa ciężar wykazania, że wystąpiły okoliczności,

za które nie ponosi odpowiedzialności i tym samym nie jest zobowiązany płacić za błędy spółki.

Są to następujące sytuacje:

- we właściwym czasie zgłoszono wniosek o ogłoszenie upadłości lub w tym samym czasie wydano postanowienie o otwarciu postępowania restrukturyzacyjnego albo o zatwierdzeniu układu w postępowaniu w przedmiocie zatwierdzenia układu;
- niezgłoszenie wniosku o ogłoszenie upadłości nastąpiło nie z jego winy;
- pomimo niezgłoszenia wniosku o ogłoszenie upadłości oraz niewydania postanowienia o otwarciu postępowania restrukturyzacyjnego albo niezatwierdzenia układu w postępowaniu w przedmiocie zatwierdzenia układu wierzyciel nie poniósł szkody.

W obszarze prawa karnego trzeba mieć na uwadze, że za korupcję menadżerską członek zarządu jest narażony na karę pozbawienia wolności do 5 lat, a w przypadku nadużycia uprawnień lub niedopełnienia ciężącego obowiązku, skutkującego wyrządzeniem spółce szkody przekraczającej 1 mln zł – do 10 lat.

Dodatkowo członek zarządu ponosi odpowiedzialność karną za niezłożenie sprawozdania finansowego lub wniosku o ogłoszenie upadłości.

Członkowie zarządu powinni również pamiętać, że jeśli prowadzona przez nich spółka nie stosuje przepisów AML, naraża się na konsekwencje administracyjne i finansowe.

Jest to jedynie wrywkowy zbiór możliwych reżimów odpowiedzialności. Bez wątplenia od osób zajmujących wyższe stanowiska kierownicze (menadżerskie) w organizacji wymaga się zachowania należytej staranności w działaniu.

Co to jest należyta staranność?

Należyta staranność została zdefiniowana w art. 355 §1 i 2 kodeksu cywilnego. Zgodnie z dyspozycją tego przepisu pojęcie to odnosi się do obowiązku zachowania staranności ogólnie wymaganej w stosunkach danego rodzaju. Przy czym pojęcie to w zakresie prowadzonej działalności gospodarczej określa się przy uwzględnieniu jej zawodowego charakteru.

Orzecznictwo wielokrotnie wypowiadało się na temat tego, czym jest przywołana należyta staranność w przypadku przedsiębiorców i jak należy ją rozumieć. Nie ma jednej sztywnej definicji tego terminu. „Staranność wymagana w stosunkach danego rodzaju będzie musiała być uwzględniana w odniesieniu do wiedzy, doświadczenia i umiejętności praktycznych, jakie wymagane są od przedsiębiorcy podejmującego się określonej działalności. Wysoki stopień staranności wymaganej od dłużnika wynika bezpośrednio z faktu, że oczekiwania osoby zawierającej z nim umowę zazwyczaj są wyższe niż w stosunku do osoby, która nie prowadzi danej działalności zawodowo”⁵⁶. Bez wątplenia na tej podstawie należy zauważyć, że od przedsiębiorcy działającego w obrocie wymaga się więcej niż od konsumenta. Jego działanie będzie zatem oceniane przez pryzmat konieczności zachowania sumienności, fachowości oraz przewidywania określonych ryzyk.

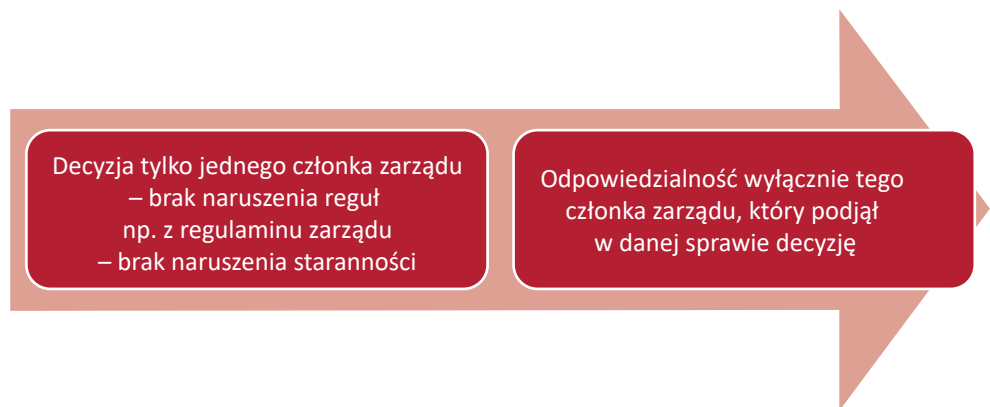
Również kadra zarządzająca jest oceniana z punktu widzenia tzw. podwyższonego miernika należytej staranności. „Staranność [ta] obejmuje, oprócz m.in. znajomości procesów organizacyjnych, finansowych, kierowania zasobami ludzkimi, także znajomość obowiązującego prawa i następstw z niego wynikających w zakresie prowadzonej działalności gospodarczej”⁵⁷.

⁵⁶ W. Borysiak, *Kodeks cywilny. Komentarz*, red. prof. K. Osajda, Warszawa 2019

⁵⁷ Por. wyrok Wojewódzkiego Sądu Administracyjnego w Szczecinie z dnia 12 października 2017 r., sygn. akt I SA/Sz 471/17

Warto zauważyć, że nawet w przypadku wewnętrznego podziału kompetencji między członkami zarządu – np. jeden członek zarządu odpowiada za działania operacyjne, pozyskiwanie kontraktów, obsługę kontrahentów, a drugi nadzoruje kwestie rozliczeń i finansów – w niektórych sytuacjach nie jest możliwe całkowite wyłączenie odpowiedzialności.

Jednak w przypadku wyraźnego rozdziału kompetencji pomiędzy członkami organu, warto uwzględnić to w schemacie organizacyjnym lub w regulaminie działalności zarządu. Może to stanowić bowiem podstawę do tzw. roszczeń regresowych – czyli jednego członka zarządu do drugiego odpowiedzialnego według wewnętrznego podziału kompetencji za dany obszar działalności, z którego powstało zobowiązanie. Indywidualizacja odpowiedzialności jest bowiem konieczna nawet w przypadku łącznego zajmowania się określonymi sprawami w myśl poniższej zamieszczonego schematu.



Przyjmuje się bowiem, że członek zarządu powinien mieć bieżącą wiedzę na temat tego, co w przedsiębiorstwie się dzieje. „Nieznajomość finansów spółki, wskazana jako przyczyna niezgłoszenia wniosku o jej upadłość, nie jest okolicznością uzasadniającą zwolnienie prezesa zarządu z odpowiedzialności za zaległości podatkowe na podstawie art. 116

ustawy z dnia 29 sierpnia 1997 r.” – Ordynacja podatkowa (jednolity tekst: Dz.U. z 2005 r. Nr 8, poz. 60 z późn. zm.)⁵⁸.

Mając to na uwadze, kadra kierownicza powinna być szczególnie zainteresowana wprowadzeniem wewnętrznych mechanizmów zarządzania zgodnością. To ona bowiem ma bardzo szeroką odpowiedzialność i jest narażona na wiele potencjalnych ryzyk. Dodatkowo, zgodnie z powszechnie obowiązującymi przepisami, od kadry menadżerskiej wymaga się bardzo dużo – nie tylko wiedzy w zakresie prowadzonej działalności, ale także znajomości prawa i podatków czy stanu finansowego organizacji. Często menadżerowie nie zdają sobie w ogóle sprawy, że określone sytuacje są penalizowane lub też mogą stanowić potencjalny obszar do ponoszenia odpowiedzialności prawnej.

Doskonałym przykładem może być tutaj wspomniane powyżej przekupstwo menadżerskie, o którym mowa w art. 296a kodeksu karnego. Przepis reguluje zjawisko tzw. korupcji w sektorze prywatnym. Kadra zarządzająca powinna zatem mieć świadomość, że podobne kwestie dotyczą nie tylko obszaru publicznoprawnego, jak zwyczajowo jest to kojarzone. Istotne jest, że penalizacji podlega również łapownictwo bierne, polegające na przyjęciu korzyści majątkowej w zamian za nadużycie uprawnień lub niedopełnienie obowiązku, co może wyrządzić przedsiębiorstwu szkodę.

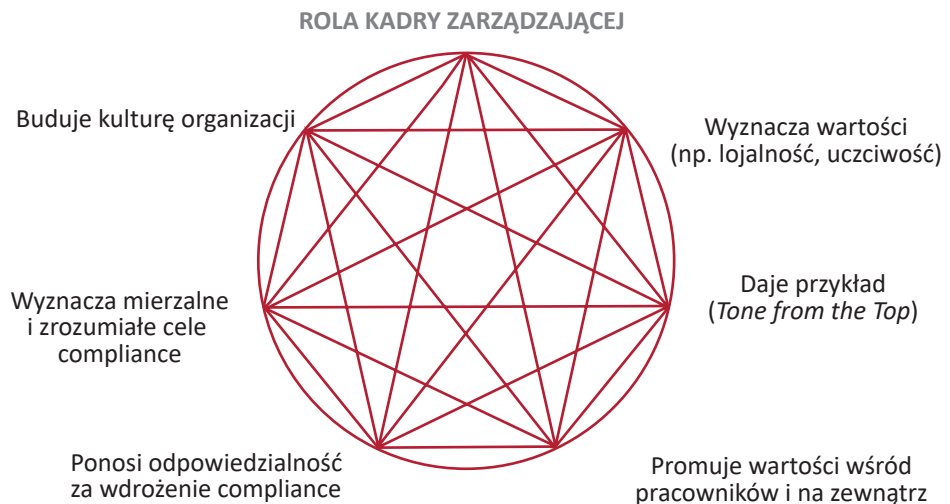
2.3. Kadra zarządzająca na straży wartości etycznych

Nie tylko chęć ograniczenia swojej odpowiedzialności jest motywacją kadry zarządzającej do wprowadzenia systemu compliance w przedsiębiorstwie. Stanowi ją także potrzeba wyznaczania zasad i wartości etycznych, z którymi

⁵⁸ Por. wyrok Sądu Najwyższego z dnia 15 maja 2014 r., sygn. akt II CSK 446/13

powinna być utożsamiana firma. I to zarówno wśród pracowników, jak i w relacjach z klientami i kontrahentami.

Istotnym filarem programu compliance jest zatem wcześniejsze wyznaczenie przez kadre zarządzającą wartości etycznych skierowanych na działanie konkretnej organizacji i dopasowanych do profilu działalności.



Ważne jest to, aby z wprowadzanymi zasadami utożsamiali się wszyscy członkowie organizacji. Powinny być one być promowane i stosowane przez kadre zarządzającą w codziennym biznesowym funkcjonowaniu. Tylko w ten sposób uda się uzyskać efekt stabilności i faktycznego stosowania w kulturze organizacji. Najczęściej wartości te funkcjonują jako kodeks etyczny przedsiębiorstwa (*Code of Conduct, Code of Ethics*) i są niejako źródłem najważniejszych informacji.

3. Funkcjonowanie systemu compliance

w przedsiębiorstwie: analiza ryzyka, wdrożenie, weryfikacja. Funkcja compliance officera

System compliance powinien być spójny i zupełny, aby mógł być efektywny. Nie jest możliwe stworzenie mechanizmów zachowania zgodności o charakterze standardowym – zawsze powinny być to rozwiązania szyte na miarę konkretnej organizacji. Tylko w takim przypadku będą one stosowane, a co za tym idzie – przyniosą oczekiwane korzyści, np. uniknięcie strat wizerunkowych poprzez wykrycie nieprawidłowości i przeprowadzenie wewnętrznego dochodzenia po zgłoszeniu sygnalisty. Proces wdrażania compliance jest długotrwały i składa się na niego wiele aspektów. „Sam system compliance spełniać musi określone wymagania. [...] nie jest wystarczające wprowadzenie jakiegokolwiek systemu compliance. Decydująca jest implementacja dobrego, efektywnego i wydajnego systemu zarządzania zagadnieniami prawnymi i etycznymi, który zapewnić będzie poprzez stosowanie dopasowanych i długofalowych środków realizację w przedsiębiorstwie celów compliance”⁵⁹.

Jak już wcześniej wspomniano, skuteczny system compliance nie jest zatem mierzony liczbą obowiązujących procedur czy innych dokumentów wewnętrznych, tylko ich faktycznym stosowaniem.

⁵⁹ Prof. B. Makowicz, *ibidem*.

Mając to na uwadze, można zaproponować następujące *to-do list*, które może stanowić podpowiedź dla przedsiębiorców chcących rozpocząć wdrażanie compliance w swoich organizacjach.



3.1. Budowa kultury organizacji

Compliance in action to najbardziej pożądanym model systemu zarządzania zgodnością. Przygotowywany w pośpiechu będzie stanowił jednak jedynie koszt, a nie korzyść. Podstawą jest bowiem zawsze wypracowanie odpowiedniej kultury organizacji, co jest procesem czasochłonnym.

Podstawowym przykładem sytuacji niepożądanych, w których nie została wypracowana kultura compliance, jest negatywny stosunek kadry zarządzającej do tego zagadnienia. Trudno mówić o jakimkolwiek systemie zarządzania zgodnością, jeśli zarząd spółki w sposób jawny go nie przestrzega oraz wyraża swój negatywny stosunek, traktując jako niepotrzebny formalizm.

Projekt wspomianej już nowej ustawy o odpowiedzialności podmiotów zbiorowych za czyny zabronione pod groźbą kary wskazuje jako istotny czynnik, mogący nawet wyłączyć odpowiedzialność danego przedsiębiorstwa – tzw. odpowiednią organizację. Konkretnie chodzi tu o:

- określenie zakresu odpowiedzialności organów, komórek organizacyjnych oraz poszczególnych osób;
- określenie zasad postępowania na wypadek zagrożenia popełnienia czynu zabronionego lub skutków niezachowania reguł ostrożności (procedura wewnętrzna);
- wyznaczenie konkretnej osoby (*compliance officer*) lub komórki organizacyjnej nadzorującej przestrzeganie przepisów i zasad regulujących działalność podmiotu zbiorowego.

Jednak nawet formalne wprowadzenie schematu organizacyjnego, zasad rozdziału kompetencji poszczególnych działów, utworzenie stanowiska osoby odpowiedzialnej za przestrzeganie systemu compliance będzie bezskuteczne w momencie, w którym nie podąży za tym „mentalność” organizacji. W praktyce będzie to związane przede wszystkim z koniecznością regularnych szkoleń dla pracowników, ale także z promowaniem określonych postaw wzorcowych – przede wszystkim właśnie przez kadrę kierowniczą. Jak już zostało wspomniane, to jej bowiem przypisuje się kluczową rolę.

3.2. Sprawdzenie istniejących rozwiązań

Wprowadzenie compliance powinno być zawsze poprzedzone zweryfikowaniem aktualnych rozwiązań w przedsiębiorstwie (*due diligence*). Częstym błędem jest tworzenie abstrakcyjnych mechanizmów, które są oderwane od rzeczywistości danej organizacji. Audyt obowiązujących procedur zakłada przede wszystkim weryfikację ich przydatności pod kątem stosowania. W tym kontekście warto odpowiedzieć sobie na dosyć prozaiczne, ale istotne pytania. Czy procedury, które obowiązują w organizacji, są napisane przystępnym językiem? Kto został z nimi zapoznany? Kto powinien ich przestrzegać? Czy są one wystarczająco konkretne? Czy nie wykluczają się wzajemnie?

Ten etap źródłowy jest bardzo istotny. Od niego zależy to, w jakim kierunku będzie zmierzała organizacja.

Warto cały czas pamiętać o tym, że sposób podejścia do tematyki compliance w dużym stopniu zależy od nastawienia kadry kierowniczej do tego zagadnienia. Jeżeli zatem zarząd jest przekonany o znakomitości obowiązujących rozwiązań i jest do nich przywiązany – niezależnie od tego, czy są one wartościowe, czy też nie – nie będzie raczej zainteresowany wprowadzeniem zmian czy usprawnień. Może bowiem utożsamiać je z krytyką swojego dotychczasowego modelu zarządzania. Jest to oczywiście błędne rozumowanie, ponieważ compliance zakłada przede wszystkim maksymalizację ochrony przedsiębiorcy na wypadek nieprawidłowości, w tym także – czy nawet przede wszystkim – ochronę kadry zarządzającej jako ponoszącej z reguły najszerzą odpowiedzialność.

3.3. Analiza ryzyka

Ten etap zakłada weryfikację obszarów, które organizacja uznaje za ryzykowne, czyli takie, w których mogą wystąpić nieprawidłowości⁶⁰. Chodzi tu rzecz jasna także o takie obszary, w których do nieprawidłowości dochodziło już wcześniej.

Przy analizie ryzyka koniecznym jest pogrupowanie sektorów działalności oraz przypisanie im progu istotności. Można wyróżnić następujące obszary prawno-podatkowe, które powinny stanowić punkt zainteresowania przy wdrażaniu compliance:

- prawo korporacyjne,

⁶⁰ Należy podkreślić, że nie chodzi tu o instytucje finansowe, w których proces analizy ryzyka może wyglądać odmiennie. Skupiamy się wyłącznie na szeroko rozumianym sektorze prywatnym, w którym działają mali i średni przedsiębiorcy.

- prawo kontraktowe,
- prawo pracy,
- przeciwdziałanie praniu pieniędzy i finansowaniu terroryzmu,
- raportowanie schematów podatkowych (MDR),
- RODO i cyberbezpieczeństwo,
- audyt,
- upadłość,
- podatek CIT,
- podatek VAT,
- akcyza i cło,
- podatek od nieruchomości.

Każdy z tych obszarów powinien zostać wzięty pod uwagę przy rozpoznaniu ryzyka.

Przykłady:

- 1) Przedsiębiorca zawiera w ramach swojej działalności gospodarczej co najmniej kilkanaście umów miesięcznie. Są to kontrakty o różnej wartości oraz z różnymi podmiotami, zawierane na różny okres. Część to umowy na dostawę półproduktów od różnych producentów z kilku krajów, o zmiennych parametrach gwarancyjnych. Pozostałe umowy są zawierane z kontrahentami. Przedsiębiorca ma również wielu klientów, także z kilku krajów.
- 2) Przedsiębiorca ma jednego stałego dostawcę półproduktów oraz jednego stałego klienta, z którym ma zawartą wieloletnią umowę o współpracy zakładającą waloryzację wynagrodzenia. Zna obydwie podmioty oraz osoby wyznaczone do realizacji umów osobiście.

W pierwszym przykładzie z uwagi na dużą liczbę zawieranych umów oraz zmienne parametry – czyli różne kraje pochodzenia, zmienna waluta, różny czas trwania umów itd. – ryzyko wystąpienia potencjalnych

nieprawidłowości przy realizacji kontraktów jest zdecydowanie większe niż w drugim przykładzie. Przedsiębiorca przywołany wcześniej powinien zabezpieczyć się na wypadek takich ryzyk poprzez wprowadzenie mechanizmów kontroli kontrahentów oraz dostawców.

Przykład:

Koncern z kapitałem amerykańskim chce rozpocząć działalność w Polsce. W tym celu zakłada spółkę z ograniczoną odpowiedzialnością. Na stanowisko prezesa zarządu powołuje osobę wyłonioną w ramach konkursu. Jest to osoba z zewnątrz, czyli taka, która nie pracowała wcześniej w tym koncernie. W spółce nie zostały ustanowione żadne ograniczenia wewnętrzne dotyczące działalności prezesa zarządu. Ma on co do zasady pełną swobodę przy zawieraniu umów oraz prowadzeniu spraw spółki.

W tym przykładzie jako istotne ryzyko należy wskazać duży zakres swobody prezesa zarządu przy uwzględnieniu potencjalnie małej wiedzy wspólnika spółki, czyli amerykańskiego koncernu, który nie ma jeszcze doświadczenia na rynku polskim. Jest to więc potencjalne pole do nadużyć. Spółka powinna uregulować wewnętrznie i skonkretyzować zakres działania, np. przy podejmowaniu kluczowych decyzji, dla których na przykład byłaby wymagana każdorazowo zgoda wspólnika. Dodatkowo spółka powinna dla transparentności przyjąć schemat organizacyjny.

Tym samym warto podkreślić, że podstawą dla compliance jest zawsze analiza sytuacji danego przedsiębiorcy. Będzie to determinował m.in. rozmiar danego przedsiębiorcy, przedmiot działalności i skala jej prowadzenia, liczba pracowników oraz przychody.

3.4. Przygotowanie dedykowanych narzędzi i procedur. Funkcja compliance officera

Z przeprowadzonego etapu weryfikacji już istniejących mechanizmów zarządzania ryzykiem, w tym procedur, oraz analizy ryzyka powinno wynikać, co organizacji jest potrzebne w obszarze compliance. Obie fazy mogą zostać ujęte w tzw. *red flag report*, czyli podsumowaniu zawierającym najbardziej newralgiczne i najpilniejsze punkty, które wymagają regulacji (patrz: przykład przedsiębiorcy zawierającego szereg różnych kontraktów).

W ślad za tym jest konieczne przygotowanie dedykowanych narzędzi i procedur. Przy czym określenie procedury powinno zostać ujęte w cudzysłów. Nie chodzi bowiem o to, aby każde zjawisko występujące w organizacji zostało ujęte w jakieś formalne ramy w postaci wielostronicowego dokumentu. O wiele istotniejszy jest przecież wspomniany już wielokrotnie aspekt praktyczny.

Kontynuując podział obszarowy z fazy analizy ryzyka, można byłoby wzorcowo wyróżnić następujące mechanizmy lub procedury warte uregulowania, a w niektórych przypadkach wprost wymagające zrobienia tego z uwagi na obowiązek prawny w tym zakresie wynikający np. z AML czy MDR:

- prawo korporacyjne:
- kodeks etyczny,
- schemat organizacyjny,
- regulamin zarządu,
- ład korporacyjny,
- kontrola organów,
- gromadzenie, weryfikacja, obieg oraz przechowywanie informacji i dokumentacji,
- konflikt interesów,

- kontrola komórek (osób sprawujących nadzór nad compliance),
- ubezpieczenie D&O dla członków zarządu;
- prawo kontraktowe:
- polityka udzielania rabatów,
- wybór i weryfikacja kontrahentów,
- procedura antykorupcyjna (przyjmowanie prezentów, rejestr korzyści);
- prawo pracy;
- przeciwdziałanie praniu pieniędzy i finansowaniu terroryzmu;
- raportowanie schematów podatkowych;
- RODO i cyberbezpieczeństwo;
- audyt;
- upadłość;
- podatek CIT;
- podatek VAT;
- akcyza lub cło;
- podatek od nieruchomości.

Wprowadzenie procedur w powyższych obszarach ma na celu ochronę organizacji przed wystąpieniem nieprawidłowości, a nie utrudnianie jej funkcjonowania. Dlatego listę tę należy traktować jako propozycję, która będzie podlegała odpowiednim zmianom w zależności od ryzyk występujących w przedsiębiorstwie.

Nie jest możliwe szczegółowe omówienie wszystkich wskazanych procedur i tego, co powinny one zawierać. Warto przyjrzeć się jednak kilku z nich.

Najważniejsze zasady i normy postępowania przedsiębiorstwa będą zawarte najczęściej w kodeksie etycznym (ang. *Code of Conduct*), który stanowi niejako punkt wyjścia dla funkcjonowania danej firmy – zarówno na zewnątrz, czyli w relacjach z klientami, jak i do wewnątrz, czyli

w relacjach między pracownikami. Kodeks etyczny zawiera model wartości, którymi kieruje się firma. Jego sformułowania są ogólne. Często w obrębie grup kapitałowych jest to jeden wspólny dokument dla wszystkich spółek wchodzących w skład grupy. Chodzi o to, aby wyznaczyć jeden wspólny azymut. Kodeksy etyczne najczęściej są dokumentami jawnymi i udostępnia się je na stronach internetowych przedsiębiorstwa czy grupy kapitałowej. Ma to być jasny sygnał dla potencjalnego klienta lub kontrahenta, że firma stosuje compliance i działa zgodnie z prawem.

W kodeksach etycznych są zawarte zasady i wartości m.in. z następujących obszarów:

- uczciwość w biznesie oraz wewnątrz organizacji (korupcja, przestrzeganie prawa, konflikt interesów),
- komunikacja, bezpieczeństwo danych,
- społeczeństwo i środowisko.

Kodeks etyczny jest ważny z punktu widzenia kadry zarządzającej, ponieważ dotyczy on całej firmy.

Innymi regulacjami, które często są wdrażane w przedsiębiorstwach, są te dotyczące szeroko rozumianej organizacji, czyli podziału zadań pomiędzy poszczególnymi osobami i działami w firmie. Umożliwia to przyporządkowanie kompetencji i ustalenie zakresu odpowiedzialności za dany obszar. Przedsiębiorcy nieposiadający takiego podziału kompetencji muszą liczyć się z tym, że na przykład w razie kontroli trudno będzie wykazać, kto był odpowiedzialny za realizację danego projektu i związane z nim czynności. Istotne w tym kontekście jest także regulowanie zasad przechowywania dokumentów i gromadzenia informacji. Jest to ważne nie tylko z praktycznego punktu widzenia (np. możliwość sprawnego wyszukania określonego dokumentu), ale także z punktu widzenia ochrony informacji oraz danych.

Przykładowo ustawa o przeciwdziałaniu praniu pieniędzy i finansowaniu terroryzmu przewiduje, że instytucje obowiązane przechowują przez okres 5 lat, licząc od pierwszego dnia roku następującego po roku, w którym zakończono stosunki gospodarcze z klientem lub w którym przeprowadzono transakcje okazjonalne:

- kopie dokumentów i informacje uzyskane w wyniku stosowania środków bezpieczeństwa finansowego;
- dowody potwierdzające przeprowadzone transakcje i ewidencje transakcji, obejmujące oryginalne dokumenty lub kopie dokumentów konieczne do identyfikacji transakcji.

Oznacza to, że przedsiębiorcy podlegający przepisom tej ustawy muszą pamiętać o tym okresie. Tym samym powinni mieć wdrożone wewnętrzne regulacje, które umożliwią przestrzeganie tego obowiązku.

Coraz częściej regulowanym obszarem jest także aspekt antykorupcyjny. Przedsiębiorcy decydują się na wprowadzenie granic kwotowych dla przyjmowania oraz wręczania prezentów kontrahentom oraz na prowadzenie tzw. rejestru korzyści, co ma eliminować problem nadużywania swoich uprawnień w celu osiągnięcia korzyści.

Niewątpliwie istotną dziedziną w kontekście wewnętrznych regulacji jest także proces weryfikacji kontrahentów. Obecnie przedsiębiorcy mają możliwość pozyskania szeregu informacji na temat swoich potencjalnych kontrahentów – na przykład w przypadku spółek będzie to sprawdzenie danych zawartych w Krajowym Rejestrze Sądowym łącznie ze sprawozdaniem finansowym i weryfikacją, czy kontrahent znajduje się na tzw. białej liście podatników, czy w Centralnym Rejestrze Beneficjentów Rzeczywistych. Należyta weryfikacja kontrahentów powinna stanowić standard i zapewniać przedsiębiorcy ochronę, np. przed ich niewyptacalnością.

Warto w tym miejscu wspomnieć też o przywołanym wcześniej Ubezpieczeniu Directors and Officers (D&O), które może stanowić dodatkowe zabezpieczenie dla kadry zarządzającej. Ubezpieczenie to standardowo chroni spółkę oraz członków zarządu przed osobistą odpowiedzialnością za roszczenia kierowane na przykład przez udziałowców, kontrahentów czy wierzycieli w związku z nieprawidłowym zachowaniem lub beczynnością w sytuacji, gdy określone działanie jest wymagane. Ubezpieczenie to jest dedykowane nie tylko członkom zarządu czy członkom rad nadzorczych, ale też np. pozostałym osobom pełniącym funkcje zarządcze lub nadzorcze, w tym osobom odpowiedzialnym za prowadzenie ksiąg rachunkowych.

Ubezpieczenie dotyczy ochrony na wypadek sytuacji, w których szkoda nastąpiła na skutek braku należytej staranności, poprzez naruszenie zaufania, przekroczenie umocowania, działanie na szkodę spółki, złożenie fałszywego oświadczenia lub oświadczenia wprowadzającego w błąd, naruszenie praw pracowniczych itp. Warto jednak zaznaczyć, że D&O nie chroni przed odpowiedzialnością karną.

W kontekście wymaganych procedur na uwagę zasługuje także funkcja compliance officera, który coraz częściej jest powoływany w przedsiębiorstwach. Co prawda najczęściej dzieje się to w podmiotach o złożonej strukturze i z kapitałem zagranicznym, ale w związku z projektem ustawy o odpowiedzialności podmiotów zbiorowych za czyny zabronione pod groźbą kary, może stać się obszarem zainteresowania znacznie szerszego grona firm.

Compliance officer to zawód, który nie jest uregulowany prawnie. Funkcja ta może być umiejscowiona w różny sposób w strukturze organizacyjnej przedsiębiorstwa. W przypadku bardziej złożonych struktur (np. spółka z kapitałem zagranicznym) najczęściej powołuje się tzw. *Chief Compliance*

Officer, który podejmuje działania centralne i koordynuje zadania lokalnych compliance officerów powoływanych w spółkach-córkach.

Funkcja compliance officera ma charakter interdyscyplinarny. Istotne jest to, aby posiadał on zarówno wiedzę, jak i był wyposażony w odpowiednie kompetencje w ramach struktury przedsiębiorstwa⁶¹. Wskazane jest, żeby compliance officer posiadał wiedzę po pierwsze z zakresu funkcjonowania przedsiębiorstwa, ale także prawa czy kwestii ekonomicznych. Musi wiedzieć, w obrębie jakich regulacji się porusza. Często zgłaszane nieprawidłowości mogą mieć bowiem charakter naruszenia przepisów prawnych.

Jak wspomniano, ważna jest pozycja compliance officera w strukturze przedsiębiorstwa. Powinien on mieć zagwarantowaną niezależność z uwagi na to, że jest ona koniecznym warunkiem do prowadzenia skutecznych dochodzeń wewnętrznych. Z reguły compliance officer o podejmowanych działaniach będzie raportował do zarządu. To na kadrze kierowniczej ciąży bowiem główny obowiązek, aby zapewnić zgodność działania przedsiębiorstwa z prawem. W swojej bieżącej pracy compliance officer musi jednak mieć legitymację także do tego, aby móc pozyskiwać określone dokumenty czy żądać wyjaśnień. Z pewnością dużym wyzwaniem dla compliance officerów będzie dostosowanie się do wymogów Dyrektywy o ochronie osób zgłaszających przypadki naruszenia prawa Unii, przyjętej przez Parlament Europejski i Radę. Jednym z jej założeń jest zapewnienie sygnalistom bardzo szerokiej ochrony, m.in. anonimowości⁶².

⁶¹ M. Haase, *Officer „compliance” jako zawód* [w:] Monitor Prawniczy 2013, Nr 13.

⁶² W przypadku gdy osobę, która złożyła doniesienie, spotkają represje, trzeba będzie jej zagwarantować dostęp do bezpłatnych porad i odpowiednich środków ochrony prawnej (np. środków mających na celu powstrzymanie mobbingu lub uniemożliwienie zwolnienia).

Przykładowe kompetencje compliance officera:

- podejmowanie działań dotyczących wdrożenia systemu zarządzania zgodnością w przedsiębiorstwie (w tym analiza ryzyka),
- odbiór zgłoszeń o nieprawidłowościach,
- przeprowadzanie wewnętrznych dochodzeń w wyniku zgłoszenia o nieprawidłowościach,
- raportowanie do kadry kierowniczej o podejmowanych działaniach oraz o efektach przeprowadzonych postępowań (względnie uzgadnianie propozycji podejmowanych działań),
- podejmowanie czynności w zakresie szerzenia świadomości compliance wśród pracowników.

Kształt i zakres kompetencji compliance officera zależy od struktury i wielkości danego przedsiębiorcy.

W obliczu dynamicznie zmieniającego się środowiska prawnego powoływanie compliance officera będzie bez wątpienia coraz popularniejsze w polskich przedsiębiorstwach.

3.5. Wdrożenie i co dalej?

Jednym z nieodzownych kroków, które powinien podjąć przedsiębiorca chcący zapewnić skuteczność systemu compliance, jest wdrożenie wcześniej przygotowanych procedur czy mechanizmów.

Wdrożenie ma dwa aspekty:

- formalny – oficjalne przyjęcie dokumentu jako obowiązującego w przedsiębiorstwie;
- faktyczny – zapoznanie z treścią dokumentu pracowników oraz podjęcie czynności o charakterze szkoleniowym mających za zadanie doprowadzenie do przestrzegania jego zapisów.

Przykładowo procedura wewnętrzna zgodnie z przepisami ustawy o przeciwdziałaniu praniu pieniędzy i finansowaniu terroryzmu powinna zostać zaakceptowana przez kadre kierowniczą wyższego szczebla.

Oba aspekty wdrożenia są tak samo ważne. Formalne przyjęcie oznacza, że w przedsiębiorstwie dany mechanizm funkcjonuje i że należy go przestrzegać. Przy czym adresaci określonych dokumentów mogą być różni. Regulamin zarządu nie jest dokumentem skierowanym na przykład do pracowników produkcyjnych, bo nie dotyczy ich zakresu zadań. Przedsiębiorcy powinni respektować również aspekt faktycznego wdrożenia, ponieważ tylko dzięki niemu osoby zainteresowane będą miały wiedzę o tym, że określony dokument w ogóle istnieje i że są zobowiązane do jego przestrzegania.

Faktyczne wdrożenie przekłada się zatem na praktyczne stosowanie. Nawet najlepiej wymyślony np. mechanizm kontrolny w ramach przedsiębiorstwa nie zadziała, jeżeli zostanie pominięty etap praktycznego stosowania. Etap ten powinien być wspierany szkoleniami dla pracowników.

Na przykład wdrożenie w przedsiębiorstwie procedury ochrony osób zgłaszających nieprawidłowości bez jednoczesnego zapewnienia mechanizmu odbioru zgłoszeń oraz ich sprawdzania, nie będzie miało wymiaru praktycznego. W teorii pracownicy będą bowiem mieli możliwość zgłoszenia nieprawidłowości, ale nie będzie jasne, kto i na jakich zasadach miałby je rozpoznać.

Elementem, którego nie wolno pomijać, jest ponadto cykliczna weryfikacja stosowania systemu compliance. W określonych odstępach czasu przedsiębiorca powinien sprawdzać, czy wdrożone mechanizmy funkcjonują. Weryfikacja ta będzie miała charakter audytu przeprowadzonego albo w ramach samej organizacji (np. przez compliance

officera), albo przez zewnętrznego audytora. Weryfikacja może polegać na przeprowadzeniu wywiadów z pracownikami oraz na sprawdzeniu dokumentów obowiązujących w ramach compliance. Wnioski płynące z audytu powinny być dla kadry zarządzającej bodźcem do dokonania ewentualnych zmian.

Dobrym sprawdzianem dla przedsiębiorcy może być sytuacja kontroli. W dobrze przygotowanej firmie pracownicy będą znali swój zakres kompetencji. Będzie wiadomo, kto jest odpowiedzialny za przechowywanie i zabezpieczenie określonych dokumentów oraz kto i w jakim zakresie jest uprawniony do udzielania informacji.

Przedstawione powyżej funkcjonowanie systemu compliance w przedsiębiorstwie stanowi jedynie propozycję. Przedsiębiorca zawsze powinien mieć na uwadze, że sprawnie działające mechanizmy zapewnienia zgodności nigdy nie będą stanowiły dla firmy niepotrzebnego balastu, lecz ochronę. Dlatego przy wdrażaniu systemów CMS tak istotne jest zachowanie wszystkich poszczególnych kroków oraz świadomość, że jest to proces, czasem nawet długotrwały, który wymaga zbudowania odpowiedniej kultury organizacji.

Rozdział 5. Compliance w prawie pracy

Autor: Klaudia Kiempa-Kamińska

W zależności od profilu działalności przedsiębiorstwa obszary ryzyka, w których jest konieczne wprowadzenie odpowiednich procedur i polityk, mogą być różne. Tym niemniej niektóre z nich niemal zawsze będą wspólne. Jednym z takich wspólnych obszarów jest prawo pracy.

Rozważając zagadnienia z tego zakresu w kontekście compliance, należy zastanowić się nad funkcją, jaką system zarządzania zgodnością powinien tutaj pełnić.

Z jednej strony compliance w prawie pracy pełni funkcję zewnętrzną. Chodzi o to, że osoby, które będą rozważać podjęcie zatrudnienia u danego pracodawcy, mogą być zainteresowane tym, czy posiada on system zarządzania zgodnością, tj. np. procedury antymobbingowe i równego traktowania, z zakresu BHP, co ma istotny wpływ na komfort i bezpieczne warunki pracy. Co więcej posiadanie tego rodzaju systemów, ale przede wszystkim ich efektywność, powinna pozytywnie wpłynąć na postrzeganie organizacji jako wiarygodnego i atrakcyjnego pracodawcy, co nabiera szczególnego znaczenia, jeżeli weźmiemy pod uwagę fakt, iż od kilku lat mamy do czynienia z tzw. rynkiem pracownika.

Z drugiej strony compliance pełni funkcję wewnętrzną, którą należy rozumieć jako usystematyzowanie działań wewnątrz organizacji mających na celu minimalizowanie ryzyka naruszeń w obszarze prawa pracy, które mogą

skutkować różnego rodzaju odpowiedzialnością, np. odszkodowawczą lub w niektórych przypadkach karną. Chodzi tu m.in. o odpowiedzialność karną za złośliwe lub uporczywe naruszanie praw pracowniczych (art. 217 kodeksu karnego), odpowiedzialność finansową za wykroczenia przeciwko prawom pracowniczym (grzywna może wynieść do 30 000 zł) czy odpowiedzialność administracyjną (kary finansowe nakładane przez Państwową Inspekcję Pracy – PIP). Poza wskazaną wyżej odpowiedzialnością nie można jednak zapomnieć, że równie istotne jest to, iż compliance w ujęciu wewnętrznym ma także wpływ na wzrost wydajności i zadowolenia wśród załogi. Oba te obszary są równie ważne i powinny być ze sobą kompatybilne.

Panuje dosyć powszechne przekonanie, że compliance w prawie pracy to **przede wszystkim polityka antymobbingowa**. Oczywiście, jest to jedna z ważniejszych procedur, która powinna być wdrożona w organizacji, niemniej nie jest to jedyny obszar wymagający uregulowania. Co, compliance w prawie pracy to nie tylko procedury, lecz także szeroko rozumiana działalność nakierowana na osiągnięcie zgodności z przepisami z zakresu prawa pracy, które nie zawsze muszą być zapisane jako konkretna polityka czy strategia. Chodzi tu w szczególności o zasady rekrutacji i zatrudniania pracowników, ochronę danych osobowych zatrudnionych w przedsiębiorstwie, wprowadzanie aktów wewnętrznych wymaganych przez przepisy prawa, jak np. regulamin pracy czy regulamin wynagradzania. W niniejszym rozdziale dokonano zwięzłego przedstawienia najważniejszych polityk oraz dokumentów wewnętrznych z punktu widzenia właściwego funkcjonowania organizacji.

1. Compliance w procesie rekrutacji

Na gruncie prawa pracy, czy też szerzej – prawa Human Resources (HR), wdrożenie odpowiednich procedur powinno zacząć się już na etapie

rekrutowania nowych pracowników. W tym zakresie chodzi oczywiście o przestrzeganie zasad uczciwej i transparentnej rekrutacji oraz sprawne przeprowadzenie kandydatów przez jej przebieg. W powyższym kontekście będzie chodziło jednak nie tyle o ryzyko naruszeń jako takie – choć zawsze należy pamiętać o kwestii dyskryminacji w procesie rekrutacji, która może mieć miejsce, o czym więcej w dalszej części rozdziału – ile bardziej o wizerunek przedsiębiorcy jako pracodawcy na rynku pracy. W tym zakresie ważne jest, aby dopilnować kwestii najbardziej podstawowych ze względu na dobre praktyki rynkowe w rekrutacji, tj. upewnić się, że kandydaci otrzymali informację zwrotną o wyniku procesu rekrutacji (przede wszystkim w sytuacji, gdy nie zostaną zatrudnieni), by wiedzieli, z kim odbędzie się spotkanie (np. imię, nazwisko, stanowisko osoby, z którą odbędzie się rozmowa czy test), ilu etapowa jest to rekrutacja, na jakie dokładnie stanowisko aplikują, jak będą wyglądały poszczególne etapy rekrutacji itd. Wskazane wytyczne nie są podyktowane wymogami prawnymi – nie ma bowiem żadnych przepisów, które zobowiązują pracodawcę na przykład do kontaktu z kandydatem lub do tego, aby poinformować go o tym, że nie przeszedł pozytywnie procesu rekrutacji. Wysłanie kurtuazyjnej wiadomości w stylu „Niestety w tej chwili nie możemy zaoferować Pani/Panu stanowiska, które odpowiadałoby Pani/Pana kwalifikacjom, ale chętnie pozostaniemy z Panią/Panem w kontakcie” jest zatem nieobowiązkowe. Niemniej jednak takie zachowanie należy postrzegać jako dobrą i pożądaną praktykę, która powinna być standardowo stosowana przez pracodawcę w prowadzonych procesach rekrutacyjnych i na stałe wpisać się w element wewnętrznej kultury organizacyjnej zakładu pracy.

Warto w tym kontekście zwrócić również uwagę na terminy przechowywania dokumentów rekrutacyjnych kandydatów, którzy nie zostali zatrudnieni. Zdania w tym przedmiocie nie są spójne. Ministerstwo Cyfryzacji stoi na stanowisku, że pracodawca ma prawo przechowywać

Curriculum vitae (CV) czy list motywacyjny po zakończonej rekrutacji w celach dowodowych w przypadku ewentualnych roszczeń dotyczących sposobu prowadzenia rekrutacji (np. zarzut dyskryminacji), wywodząc to z treści art. 6 ust. 1 lit. f RODO. Oczywiście czas przechowywania dokumentacji rekrutacyjnej nie jest nieograniczony i co do zasady powinien upłynąć maksymalnie w ciągu kilku miesięcy⁶³.

Z kolei Urząd Ochrony Danych Osobowych (UODO) stoi na stanowisku, że dokumenty rekrutacyjne kandydatów, którzy nie zostali zatrudnieni, powinny być niezwłocznie niszczone po podpisaniu umowy z wybraną osobą, gdyż nie ma prawnej podstawy do dalszego przetwarzania danych pozostałych kandydatów⁶⁴.

W nawiązaniu do tych sprzeczności w stanowiskach należy wskazać, że – zdaniem autorki niniejszego rozdziału – w Polsce właściwym w sprawach dotyczących ochrony danych osobowych jest Prezes UODO, który ma status i kompetencje organu nadzorczego, które zostały określone w RODO. Zatem co do zasady dokumenty niewybranego kandydata powinny zostać trwale usunięte po zakończeniu rekrutacji i wyborze innej osoby na określone stanowisko. Tym niemniej podejście zdroworozsądkowe nakazywałoby stworzenie takiej procedury, która po ocenie ryzyka wystąpienia kandydatów z ewentualnymi roszczeniami ze względu na brak zatrudnienia, będzie przewidywała mechanizm przechowywania dokumentacji rekrutacyjnej przez jakiś czas, jednak okres ten powinien być jak najkrótszy i uzasadniony okolicznościami.

⁶³ Objasnienia prawne z dnia 23.01.2019 r. wydane przez Ministra Cyfryzacji na podstawie art. 33 ustawy z dnia 6 marca 2018 r. Prawo przedsiębiorców na wniosek Rzecznika Małych i Średnich Przedsiębiorców, <https://mc.bip.gov.pl/objasnienia-prawne/objasnienia-prawne.html>.

⁶⁴ Poradnik dotyczący zatrudnienia wydany przez UODO, <https://uodo.gov.pl/pl/138/545>.

Zgodność powinna być oczywiście zapewniona również w zakresie obowiązku zawarcia właściwej umowy z pracownikiem – nie jest pożądane celowe obchodzenie formy umowy o pracę ze względów np. finansowych. Zastępowanie jej umową cywilno-prawną jest, niestety, nadal dosyć powszechną praktyką na rynku i być może na krótką metę jest ekonomicznie opłacalne dla pracodawcy. Niemniej podpisanie takiej umowy w celu obejścia przepisów prawa pracy naraża przedsiębiorcę na koszty związane np. z procesem o ustalenie istnienia stosunku pracy oraz z kontrolami ze strony PIP.

Innymi przykładami compliance na etapie rekrutacji i zatrudnienia są przestrzeganie zasad dotyczących liczby i czasu trwania umów zawieranych na czas określony bądź okres próbny czy zachowanie obowiązku niezawierania z tym samym pracownikiem ponownej umowy na okres próbny na tym samym stanowisku, z tym samym zakresem obowiązków.

W dużych organizacjach, które mają w swojej strukturze departament HR, to właśnie ten dział powinien brać czynny udział w kształtowaniu kultury przedsiębiorstwa w tym zakresie i wspierać przestrzeganie przepisów prawa przez pracodawcę, dlatego istotne jest, żeby osoby pracujące w tych działach przedsiębiorstw posiadały odpowiednią wiedzę i doświadczenie, które pozwoli im sprostać wskazanym wymogom i oczekiwaniom.

1.1. Zgodność w zakresie ochrony danych osobowych

Przy okazji rozważań o rekrutacji należy zwrócić także uwagę na niezwykle gorący ostatnio i wspomniany w niniejszej publikacji temat, tj. **ochrony danych osobowych**, w szczególności w kontekście zmian, które są związane z wprowadzeniem RODO. W tym zakresie należy zwrócić uwagę na treść art. 221 kodeksu pracy. Przepis ten uległ zmianie właśnie z uwagi na wejście

w życie tego rozporządzenia. Wskazuje on katalog danych osobowych, których pracodawca może żądać od osoby ubiegającej się o zatrudnienie w organizacji (§ 1) oraz już od samego pracownika, którego wybrał (§ 2).

Danymi osobowymi, których potencjalny pracodawca może żądać od kandydata, są: imię (imiona), nazwisko, data urodzenia, dane kontaktowe, zaś ze względu na niezbędność do wykonywania pracy pracodawca może także żądać dodatkowych informacji dotyczących wykształcenia, kwalifikacji zawodowych oraz dotychczasowego przebiegu zatrudnienia. Z kolei od zatrudnionego pracownika pracodawca może żądać przekazania szerszego zakresu danych. Zgodnie z przepisami mogą to być inne dane osobowe pracownika, a także imiona i nazwiska oraz daty urodzenia jego dzieci, jeżeli podanie takich danych jest konieczne ze względu na korzystanie przez pracownika ze szczególnych uprawnień przewidzianych w prawie pracy (np. z dni opieki na dziecko) czy numeru PESEL. Oczywiście dopuszczalne jest żądanie jeszcze innych danych, jeżeli taki obowiązek wynika z odrębnych przepisów. Mowa tu na przykład o zaświadczeniu o niekaralności, które w przypadku wybranych zawodów jest niezbędne na etapie podjęcia decyzji o współpracy.

Wyjątkową uwagę pracodawca powinien także skierować na zagadnienie **monitoringu wizyjnego** w zakładzie pracy, gdyż utrwalanie i przechowywanie wizerunków pracowników oraz osób przebywających na terenie przedsiębiorstwa jest również formą przetwarzania danych osobowych. Przepis traktujący o monitoringu wizyjnym, który został wprowadzony do kodeksu pracy na podstawie przepisów o ochronie danych osobowych, jest stosunkowo nowy i wskazuje sytuacje, w których monitoring jest dopuszczalny. Ma to miejsce wtedy, kiedy ten instrument jest stosowny ze względu na niezbędność do zapewnienia bezpieczeństwa pracowników lub ochrony mienia lub kontroli produkcji lub zachowania w tajemnicy informacji, których ujawnienie mogłoby narazić pracodawcę

na szkodę (art. 222 § 1 kodeksu pracy). Z treści przepisu wynika zatem, że zasadą dla wdrożenia monitoringu są z jednej strony jego niezbędność, z drugiej zaś – ochrona godności pracownika, jego wolności i niezależności⁶⁵.

W odniesieniu do pracodawców zarówno stosowanie monitoringu, jak i procedura jego stosowania powinny wynikać z obowiązującego w zakładzie regulaminu pracy lub być uregulowane w układzie zbiorowym pracy. Jeżeli pracodawca jest zwolniony z obowiązku posiadania wskazanych wyżej dokumentów, o stosowaniu monitoringu w organizacji należy poinformować pracowników w np. obwieszczeniu, nie później jednak niż na dwa tygodnie przed rozpoczęciem jego stosowania. Co więcej każde monitorowane pomieszczenie powinno być odpowiednio oznaczone na przykład znakami informującymi o stosowaniu monitoringu w widocznym miejscu (tzw. poinformowanie uprzednie). Utrwalony obraz pracodawca, zgodnie z przepisami, może przechowywać jedynie przez 3 miesiące, chyba że nagrania mają stanowić dowód w postępowaniu. Wówczas można je przechowywać do czasu prawomocnego zakończenia postępowania.

Oczywiście nie każde pomieszczenie może być wyposażone w kamery. Przepis wprost wyłącza dopuszczalność monitoringu w pomieszczeniach udostępnianych zakładowej organizacji związkowej. Z kolei w pomieszczeniach sanitarnych (np. łazienka, toaleta), w stołówce czy w palarni monitoring wizyjny również jest niedopuszczalny, chyba że w tych miejscach jest on niezbędny ze względu na zapewnienia bezpieczeństwa pracowników, ochrony mienia, kontroli produkcji lub zachowania w tajemnicy informacji, których ujawnienie mogłoby narazić pracodawcę na szkodę i nie doprowadzi do naruszenia godności czy innych dóbr osobistych pracownika. Niemniej monitoring pomieszczeń sanitarnych

⁶⁵ Jaśkowski K., Maniewska E., *Komentarz aktualizowany do kodeksu pracy*, LEX/el. 2019.

wymaga uzyskania uprzedniej zgody zakładowej organizacji związkowej, a jeżeli u pracodawcy taka nie działa – uprzedniej zgody przedstawicieli pracowników wybranych w trybie przyjętym u danego pracodawcy (art. 222 § 2 kodeksu pracy). Odnosząc się do przesłanek dopuszczalności monitoringu pomieszczeń socjalnych ze względu na okoliczności wymienione wyżej, takie sytuacje należy zawsze oceniać *ad casum* i każdy przypadek instalowania kamer w takich miejscach należy oceniać przez pryzmat indywidualnego przypadku, który zaistniał u pracodawcy.

Kodeks pracy przewiduje także inny rodzaj monitoringu – monitoring poczty elektronicznej. Zgodnie z art. 223: „jeżeli jest to niezbędne do zapewnienia organizacji pracy umożliwiającej pełne wykorzystanie czasu pracy oraz właściwego użytkowania udostępnionych pracownikowi narzędzi pracy, pracodawca może wprowadzić kontrolę służbowej poczty elektronicznej pracownika (monitoring poczty elektronicznej)”. Tutaj katalog przesłanek jest inny niż w przypadku monitoringu wizyjnego. Nie ma w nim na przykład wymienionego bezpieczeństwa czy ochrony mienia. Przepis ten w kontekście compliance nabiera realnego znaczenia w sytuacji, w której pracodawca zdecyduje się na kontrolę służbowej skrzynki mailowej pracownika. Jest więc niezwykle istotne to, aby w wewnętrznych procedurach wyraźnie określić, że służbowy adres mailowy może być używany wyłącznie do spraw związanych z wykonywaniem obowiązków pracowniczych i nie powinno się, czy wręcz jest wyraźny zakaz, jego wykorzystywania do spraw prywatnych. Pozwoli to uniknąć sytuacji, w której pracownik nie będzie chciał udostępnić swojej skrzynki, powołując się na fakt, iż znajdują się tam także jego prywatne wiadomości. Oczywiście pracownika należy poinformować, jaka jest praktyka firmy w tym zakresie i rekomenduje się zrobienie tego w formie pisemnej.

Podobnie należy postąpić przy tworzeniu polityki dotyczącej używania laptopów czy telefonów służbowych – tam także należy wprost wskazać,

czy, w jakim zakresie i na jakich zasadach pracownik może korzystać ze sprzętów służbowych do celów prywatnych, co pozwoli uniknąć nieporozumień w razie, gdy np. pojawi się podejrzenie, że pracownik dopuszcza się nadużyć finansowych i odmawia oddania sprzętu albo nie zgadza się na jego kompleksowe przejrzanie, zasłaniając się treściami prywatnymi, które tam się znajdują.

2. Polityka antymobbingowa, niedyskryminacji i równego traktowania

Jednym z naczelných obowiązków pracodawcy, który wynika wprost z przepisów kodeksu pracy, jest obowiązek przeciwdziałania mobbingowi. Źródła umocowania dla tego obowiązku należy poszukiwać w przepisach nakazujących ochronę ludzkiej godności, tj. m.in. w samej Konstytucji Rzeczypospolitej Polskiej⁶⁶. Procedura antymobbingowa powinna być zestawem konkretnych, zorganizowanych i systematycznych przedsięwzięć podejmowanych przez pracodawcę w celu przeciwdziałania mobbingowi⁶⁷. W kontekście powyższego warto przywołać wyrok Sądu Najwyższego z dnia 3 sierpnia 2011 r., I PK 35/11⁶⁸, w którym Sąd przyjął, że przeciwdziałanie mobbingowi stanowi kontraktowy obowiązek pracodawcy, a pracodawca powinien przeciwdziałać mobbingowi, w szczególności prowadząc szkolenia dla pracowników, w trakcie których będzie informować, czym jest zjawisko mobbingu, jakie niesie ze sobą niebezpieczeństwo i konsekwencje oraz jakie stosuje procedury umożliwiające wykrycie i zwalczanie tego zjawiska⁶⁹.

⁶⁶ Baran K.W. (red.), *Kodeks pracy. Komentarz*, wyd. IV, 2018.

⁶⁷ Marciniak J., *Postępowanie antymobbingowe w zakładzie pracy*, LEX, wersja od 2014.

⁶⁸ Wyrok Sądu Najwyższego z dnia 3 sierpnia 2011 r., I PK 35/11, OSNP 2012, nr 19–20, poz. 238.

⁶⁹ Marciniak J., *Postępowanie antymobbingowe w zakładzie pracy*, LEX, wersja od 2014.

Przechodząc do definicji mobbingu zawartej w art. 943 kodeksu pracy, należy wskazać, że to pojęcie oznacza działania lub zachowania dotyczące pracownika lub skierowane przeciwko pracownikowi, polegające na uporczywym i długotrwałym nękaniu lub zastraszaniu pracownika, wywołujące u niego zaniżoną ocenę przydatności zawodowej, powodujące lub mające na celu poniżenie lub ośmieszenie pracownika, izolowanie go lub wyeliminowanie z zespołu współpracowników. Tytułem przykładu czym jest mobbing, można przytoczyć orzeczenie Sądu Apelacyjnego we Wrocławiu, który wskazał, że „mobbing może się wyrażać również w ciągłym przerywaniu wypowiedzi, reagowaniu krzykiem, ciągłym krytykowaniu i upominaniu, upokarzaniu, stosowaniu pogroźek, unikaniu rozmów, niedopuszczaniu do głosu, ośmieszaniu, ograniczeniu możliwości wyrażania własnego zdania, nieformalnym wprowadzeniem zakazu rozmów z nękanym pracownikiem, uniemożliwieniu komunikacji z innymi, a także powierzaniu prac poniżej kwalifikacji i uwłaczających, odsunięciu od odpowiedzialnych i złożonych zadań, zarzucaniu pracą, lub nie dawaniu żadnych zadań lub ich odbieraniu itp. Jednak należy podkreślić, że normalne kulturalne egzekwowanie wykonania poleceń nie stanowi mobbingu, bo podległość służbowa wynika z natury stosunku pracy”⁷⁰.

Pracodawca powinien więc podjąć działania niezbędne do zwalczania i minimalizowania ryzyka związanego z wystąpieniem mobbingu, co wymaga od niego aktywności na wielu płaszczyznach. Podkreślenia wymaga fakt, że wprowadzenie jakiegokolwiek procedury antymobbingowej – tylko dla samej idei jej wprowadzenia, a następnie bezskutecznego egzekwowania – może okazać się niewystarczające i nie pozwoli na osiągnięcie założonych celów, czyli zabezpieczenia interesów zarówno pracodawcy, jak i pracowników. Wprowadzenie procedury

⁷⁰ Wyrok Sądu Apelacyjnego we Wrocławiu Wydział III Pracy i Ubezpieczeń Społecznych z dnia 27 września 2012 r. III A Pa 27/12.

antymobbingowej powinno być podyktowane chęcią rzeczywistego wywiązania się przez pracodawcę z nałożonego na niego obowiązku i kontroli oraz minimalizowania ryzyka w tym obszarze. Konieczne w tym wypadku jest to, żeby pracownicy wiedzieli, że taka procedura została opracowana, znali jej treść lub co najmniej mieli realną możliwość zapoznania się z nią.

Przy okazji omawiania procedury antymobbingowej warto zwrócić uwagę na jeszcze jedną kwestię. Często zdarza się, że pracownicy mają niewielkie pojęcie czy wręcz żadnego o tym, czym w istocie jest mobbing. Niezrozumienie w tej materii może prowadzić do dosyć kuriozalnych sytuacji, w których pracownik za mobbing uzna fakt, który w kontekście definicji mobbingu jest zupełnie irrelevantny, np. konstruktywną krytykę ze strony przełożonego czy współpracownika, wysokie wymagania czy zlecaną dużą liczbę zadań pracownikowi, której rozmiar znajduje jednak obiektywne uzasadnienie. Takie stanowisko potwierdza orzecznictwo. I tak na przykład Sąd Apelacyjny w Katowicach wskazał, że „samo poczucie pracownika, że podejmowane wobec niego działania i zachowania mają charakter mobbingu, nie są wystarczającą podstawą do stwierdzenia, że rzeczywiście on występuje. Stwierdzenie zatem, czy nastąpiło nękanie i zastraszanie pracownika, czy działania te miały na celu i mogły lub doprowadziły do zaniżonej oceny jego przydatności zawodowej, do jego poniżenia, ośmieszenia, izolacji, bądź wyeliminowania z zespołu współpracowników, opierać się musi na obiektywnych kryteriach. Kryteria te zaś wynikają z rozsądnego postrzegania rzeczywistości, prowadzącego do właściwej oceny intencji drugiej osoby w określonych relacjach społecznych”⁷¹. Ten sam sąd wskazał, że „nawet niesprawiedliwa, lecz incydentalna krytyka pracownika nie może być kwalifikowana jako mobbing. Samo poczucie pracownika, iż podejmowane wobec niego działania

⁷¹ Wyrok Sądu Apelacyjnego w Katowicach z dnia 8 listopada 2018 r. III APa 47/18.

i zachowania mają charakter mobbingu, nie są wystarczającą podstawą do stwierdzenia, że rzeczywiście on występuje”⁷².

W tym kontekście niezwykle ważna rola przypada pracodawcy, który powinien w pierwszej kolejności zrobić rozpoznanie wśród załogi, czy i jak pracownicy rozumieją zjawisko mobbingu. W pierwszym kroku pomocne w tym zakresie mogą być ankiety dla pracowników, w których poprzez odpowiednie i umiejętnie zadane pytań pracodawca dowie się, jak jego pracownicy interpretują to pojęcie. Także szkolenia praktyczne prowadzone przez wykwalifikowane podmioty będą bardzo ważne. Wszystko po to, aby przybliżyć pracownikom problem. To z kolei oznacza, że poza wprowadzeniem samej procedury w organizacji ważną rolę pełnią działania wykonane na przedpolu mające na celu uświadomienie zjawiska. Tylko wprowadzenie kompletnej procedury, która będzie uzupełniona odpowiednim przygotowaniem, może odnieść spodziewany efekt, czyli jej pełną implementację w organizacji. Jest to istotne z tego względu, że tylko skuteczna i stosowalna praktycznie procedura antymobbingowa pozwoli na rzeczywiste zarządzanie ryzykiem na tym polu.

W kontekście skuteczności wypada jeszcze dodać jedną, bardzo ważną, a często pomijaną kwestię. Nierzadko w praktyce zdarza się, że spółka-matka z siedzibą np. w USA⁷³ narzuca swoje procedury spółkom-córkom w innych krajach, także w zakresie przeciwdziałania mobbingowi. Spółki-córki z kolei wychodzą z założenia, że w związku z tym posiadają w swojej organizacji skuteczną procedurę compliance. Jednak nic bardziej mylnego – bezrefleksyjne wdrażanie procedury antymobbingowej czy jakiegokolwiek innej z odmiennych systemów prawnych nie może odnieść

⁷² Wyrok Sądu Apelacyjnego w Katowicach z dnia 8 lutego 2018 r. III APa 74/17.

⁷³ Celowo wskazuję na Stany Zjednoczone z uwagi na to, że tam kultura dotycząca systemu zarządzania zgodnością jest obecna od wielu lat i jest wpisana w codzienne funkcjonowanie tamtejszych przedsiębiorstw.

spodziewanego skutku. Z uwagi na różne uregulowania prawne czy też kultury prawne, nie wszystkie rozwiązania zaadaptowane wprost z innych krajów będą skuteczne na gruncie polskich przepisów. Innymi słowy nie jest wystarczające samo wprowadzenie polityki antymobbingowej. Konieczne jest, żeby była ona skuteczna, a by to nastąpiło, musi znajdować oparcie w przepisach obowiązujących w miejscu, w którym znajduje się zakład pracy czy też mieć na względzie to, jakie przepisy obowiązują zatrudnionych w zakładzie pracowników. Polityka antymobbingowa, którą organizacja chce zaadaptować od spółki-matki, powinna zatem zostać dogłębnie zweryfikowana pod kątem możliwości jej zastosowania w polskim systemie prawnym. W razie potrzeby powinna ona zostać dostosowana do polskich przepisów oraz przetłumaczona na język zrozumiały dla pracowników zatrudnionych w organizacji. Proces globalizacji, a także szybki rozwój wielu branż, jak np. outsourcingu, powoduje, iż w wielu polskich firmach, czy też oddziałach zagranicznych przedsiębiorstw zlokalizowanych w Polsce, znaczna część pracowników w ogóle nie mówi po polsku. W takich przedsiębiorstwach jest konieczne zapewnienie przetłumaczenia odpowiednich dokumentów nie tylko na język polski, ale również na język zrozumiały dla każdego z pracowników. Umożliwi to rzeczywiste zapoznanie się z procedurą przez pracowników i jej efektywne stosowanie.

Przechodząc do samej treści procedury antymobbingowej należy wskazać, że zasadniczo powinna ona być zbudowana na dwóch podstawach. Z jednej strony ma opisywać procedurę skargi na wypadek zaistnienia mobbingu, z drugiej zaś – przewidywać działania zapobiegawcze⁷⁴. Przedmiotem tego dokumentu powinno być w szczególności:

- opis, jak należy rozumieć mobbing,

⁷⁴ Chakowski M., „Wewnętrzna polityka antymobbingowa” drogą do rozwiązania problemu mobbingu na poziomie zakładu pracy, Monitor Prawa Pracy 12/2010.

- wskazanie, że pracodawca podejmuje działania mające na celu przeciwdziałaniu temu zjawisku.

Procedura powinna opisywać, jak należy postępować w sytuacji, gdy osoba uzna, że jest mobbingowana w miejscu pracy (system składania skarg), tj. wskazywać kanał zgłoszenia czy osobę, którą można poinformować o sytuacji w razie podejrzenia zaistnienia mobbingu. Zaleca się, aby procedura przewidywała pisemne poinformowanie o zaistnieniu mobbingu, tak aby pozostał ślad po dokonaniu zgłoszenia. Co istotne wszyscy pracownicy powinni być zaznajomieni z procedurą składania tego rodzaju skarg.

Polityka antymobbingowa powinna także opisywać kolejne kroki, które są podejmowane po wpłynięciu skargi. Chodzi na przykład o powołanie bezstronnej komisji. Najlepiej, aby należały do niej osoby godne zaufania, które znają specyfikę organizacji, zależności ekonomiczne i personalne. Jeśli u pracodawcy działają związki zawodowe, to można powołać kogoś z organizacji związkowej. Skład komisji nie musi czy nawet nie powinien być za każdym razem taki sam. Ma to za zadanie zapewnienie bezstronności jej członków względem rozpatrywanej sprawy.

Jeśli chodzi o działania prewencyjne w organizacji, to można w tym zakresie opisać politykę szkoleniową i informacyjną dotyczącą zjawiska jakim jest mobbing, o których była mowa wyżej. Ważne jest, by szkolenia z tej tematyki były powszechne. Sytuacja idealna byłoby oczywiście wtedy, kiedy w szkoleniach brałoby udział wszyscy pracownicy, jednak może okazać się, że w większości organizacji racjonalne i możliwe będzie jedynie przeszkolenie osób z kadry kierowniczej oraz pracowników działu

kadr⁷⁵. W tym kontekście warto wspomnieć o obowiązku informacyjnym pracodawcy z art. 29 § 3 i 33 kodeksu pracy dotyczącym m.in. porządku i organizacji pracy. Przy zawieraniu umów – pracownikowi, oprócz informacji takich jak np. tygodniowa i dobową normą czasu pracy, wymiar urlopu wypoczynkowego (o ile nie zostało to już zawarte w treści umowy o pracę) – często są przekazywane także wyciągi z innych przepisów, między innymi te dotyczące mobbingu oraz równego traktowania. Właśnie wtedy można pracowników zaopatrzyć także w specjalnie przygotowane kompaktowe materiały informacyjne, jak np. broszury lub prezentacje, które opisują najważniejsze aspekty dotyczące mobbingu oraz równego traktowania. Tak przygotowane materiały będą z pewnością dużo bardziej praktyczne i przystępne w odbiorze.

Niezależnie od powyższego jest zalecane kompleksowe przeszkolenie tych osób, które mają być członkami komisji czy zespołów antymobbingowych przewidzianych w wewnętrznej procedurze⁷⁶.

Wszystkie opisane wyżej działania mają przede wszystkim na celu podniesienie świadomości – a w niektórych przypadkach po prostu uświadomienie – wśród pracowników, czym jest zjawisko mobbingu w środowisku pracy. Szkolenia nie muszą być dedykowane wyłącznie zjawisku mobbingu. Mogą także pomagać w budowaniu komunikacji między pracownikami, szeroko pojętych partnerskich relacji interpersonalnych w zespole czy w rozwiązywaniu konfliktów.

Wprowadzając politykę antymobbingową pracodawca może uniknąć wielu negatywnych skutków zarówno tych finansowych mających swe źródło np. w wypłacie odszkodowania czy poniesieniu kosztów potencjalnych

⁷⁵ Marciniak J., *Przeciwdziałanie mobbingowi w miejscu pracy. Poradnik dla pracodawcy*, Monografia, ABC 2008.

⁷⁶ *Ibidem*.

procesów, zapłaty kar nałożonych przez PIP, jak i strat niematerialnych, czyli np. utrata reputacji lub zmniejszenie efektywności pracy. Co więcej trzeba mieć na względzie, iż odpowiedzialność pracodawcy oparta na art. 943 kodeksu pracy jest oceniana przez pryzmat jego winy. Jeżeli zatem pracodawca wykaże, iż podjął działania mające na celu przeciwdziałanie mobbingowi i obiektywnie oceniając, można potwierdzić ich skuteczność, pracodawca może na tej podstawie uwolnić się od wskazanej odpowiedzialności⁷⁷.

Jak wspomniano, przeciwdziałanie mobbingowi przez pracodawcę może polegać w szczególności na szkoleniu pracowników, tzn. informowaniu o skutkach i konsekwencjach mobbingu, niebezpieczeństwie jakie ze sobą niesie czy stosowaniu procedury, która pozwoli wykryć i zakończyć to niepożądane zjawisko⁷⁸. O ile należy stwierdzić, że nawet najlepiej przygotowana procedura antymobbingowa może nie być skuteczna na tyle, żeby całkowicie wykluczyć wystąpienie zjawiska mobbingu u danego pracodawcy, o tyle wprowadzenie właściwej polityki, która spełnia warunki wyżej opisane, może uwolnić pracodawcę od negatywnych konsekwencji związanych z wystąpieniem zjawiska i skutkować odpowiedzialnością tylko konkretnej osoby, tj. sprawcy czynu mającego charakter mobbingu.

Polityka antymobbingowa nie musi być osobnym aktem. Odpowiednie zapisy dotyczące zjawiska mobbingu mogą z powodzeniem zostać dołączone na przykład do obowiązującego w zakładzie regulaminu pracy lub układu zbiorowego pracy. Dopuszczalna wydaje się również możliwość inkorporowania takich reguł do dokumentów statutowych pracodawcy, co – jak wskazują niektórzy autorzy – uczyni z zakładowej procedury antymobbingowej szczególne źródło prawa pracy zgodnie z art. 9 § 1

⁷⁷ Wyrok Sądu Najwyższego z dnia 3 sierpnia 2011 r. I PK 35/11.

⁷⁸ Jaśkowski K., Maniewska E., *Komentarz aktualizowany do Kodeksu pracy*, LEX/el. 2019.

kodeksu pracy. To z kolei wpłynie na pełniejszą realizację ustawowego obowiązku przeciwdziałania mobbingowi⁷⁹.

Kolejnym aspektem dotyczącym działań zgodnych z przepisami prawa pracy w przedsiębiorstwie jest przestrzeganie zasad równego traktowania i przeciwdziałanie dyskryminacji. Jest to drugi obok obowiązku przeciwdziałania mobbingowi nakaz kierowany pod adresem pracodawców⁸⁰.

Przepis art. 183a kodeksu pracy stanowi implementację dyrektyw wspólnotowych nakazujących równe traktowanie w zatrudnieniu. Te akty prawne nakazują równe traktowanie i walkę z dyskryminacją ze względu na płeć, pochodzenie rasowe lub etniczne, religię lub przekonania, niepełnosprawność, wiek lub orientację seksualną⁸¹. Spełnieniem obowiązku przeciwdziałania dyskryminacji w zatrudnieniu jest wprowadzenie i przestrzeganie uczciwej polityki równego traktowania, która czyni zadość obowiązkowi pracodawcy wyrażonemu w kodeksie pracy w zakresie przeciwdziałania temu niepożądanemu zjawisku. W procedurze równego traktowania – która może być albo osobnym dokumentem, albo stanowić np. część polityki antymobbingowej – można zawrzeć procedurę zgłaszania przejawów molestowania, co, zgodnie z orzecznictwem Sądu Najwyższego, wskazywałoby na spełnienie obowiązku pracodawcy w zakresie przeciwdziałania dyskryminacji. W jednym ze swoich orzeczeń Sąd ten uznał, że „pracodawca, który nie reaguje na znane mu przypadki naruszania godności i toleruje wykreowaną w miejscu pracy atmosferę zastraszania, wrogości, poniżenia lub upokorzenia wobec choćby

⁷⁹ Chakowski M., „Wewnętrzna polityka antymobbingowa” drogą do rozwiązania problemu mobbingu na poziomie zakładu pracy, *Monitor Prawa Pracy* 12/2010, do całości.

⁸⁰ Sobczyk A., *Mobbing a przeciwdziałanie mobbingowi. Dyskryminacja a przeciwdziałanie dyskryminacji*, MOPR 2015, Nr 4.

⁸¹ Walczak K., *Kodeks pracy. Komentarz* 2019, wyd. 29.

jednego pracownika, łamie art. 94 pkt 2b kp⁸², tj. narusza obowiązek przeciwdziałania dyskryminacji w zatrudnieniu.

W kontekście tego obowiązku należy mieć na uwadze to, że w sytuacji, w której pracownik zarzuci pracodawcy dyskryminacyjne traktowanie, to na pracodawcę zostaje przerzucony ciężar dowodu tego, że przy nierównym traktowaniu danego pracownika kierował się kryteriami obiektywnymi, a tym samym nie naruszył obowiązku określonego w art. 94 pkt 2b kodeksu pracy. Takie podejście potwierdza orzecznictwo Sądu Najwyższego, „pracownik powinien wskazać fakty uprawdopodobniające zarzut nierównego traktowania w zatrudnieniu, a wówczas na pracodawcę przechodzi ciężar dowodu, że kierował się obiektywnymi powodami (art. 183b § 1 kp i art. 10 dyrektywy Rady 2000/78/WE z dnia 27 listopada 2000 r. ustanawiająca ogólne warunki ramowe równego traktowania w zakresie zatrudnienia i pracy, Dz. U. UE L 303 z 2.12.2000, s. 16–22; polskie wydanie specjalne rozdział 05, Tom 04, s. 79)”⁸³.

Tym samym przyjęcie odpowiedniej polityki równego traktowania i przeciwdziałania dyskryminacji w organizacji mogłoby pomóc pracodawcy uwolnić się od odpowiedzialności za naruszenie obowiązku w tym zakresie poprzez dochowanie należytej staranności. Takim działaniem mogą być wspomniane wcześniej broszury informacyjne dla pracowników, które będą mogły stanowić jeden z dowodów przydatnych dla wykazania, iż pracodawca dochował należytej staranności na wypadek potencjalnego procesu sądowego.

⁸² Wyrok Sądu Najwyższego – Izba Pracy i Ubezpieczeń Społecznych z dnia 7 listopada 2018 r. II PK 210/17.

⁸³ Wyrok Sądu Najwyższego – Izba Pracy, Ubezpieczeń Społecznych i Spraw Publicznych z dnia 9 czerwca 2006 r. III PK 30/06.

Pracodawca powinien przeciwdziałać dyskryminacji nie tylko w trakcie zatrudnienia, ale już na etapie rekrutacji. Dokonując na przykład opisu stanowiska, należy odnieść się do kryteriów obiektywnych, wskazać obowiązki i cele bez odnoszenia się do kryteriów dyskryminacyjnych⁸⁴. Jest to istotne nie tylko z punktu widzenia odpowiedzialności pracodawcy za dyskryminowanie w procesie rekrutacji, ale ma też ogromny wpływ na wizerunek organizacji jako pracodawcy na rynku pracy.

3. Compliance w aktach wewnętrznie obowiązujących

Kodeks pracy nakłada na pracodawcę szereg obowiązków w zakresie tworzenia wewnętrznych aktów zakładowych oraz wprowadzania przepisów w organizacji, które zapewniają, że zakład działa zgodnie z obowiązującym prawem. Chodzi m.in. o wprowadzenie takich przepisów, jak np. regulamin pracy czy regulamin wynagradzania. Jest zatem istotne, aby pracodawcy, którzy zgodnie z prawem powinni mieć te akty, rzeczywiście je tworzyli, zapewniając ich należyłą treść oraz wymagany przez prawo sposób wprowadzenia, jak też zaznajamiali pracowników z ich treścią.

Regulamin pracy powinien zawierać wszystkie ustawowe wymogi określone w art. 104 kodeksu pracy, czyli m.in. opisywać organizację pracy, warunki przebywania na terenie zakładu, system czasu pracy, przepisy dotyczące pory nocnej, termin, miejsce czas i częstotliwość wypłaty wynagrodzenia, obowiązki dotyczące BHP, sposób potwierdzania przybycia i obecności pracowników w zakładzie pracy, usprawiedliwianie nieobecności w pracy itd. Co więcej, jeśli pracodawca chce wprowadzić monitoring wizyjny,

⁸⁴ Walczak K., *Dokumentacja pracownicza w procesie rekrutacji*, MOPR 2005, Nr 4.

powinien inkorporować odpowiednie zapisy dotyczące tego zagadnienia do regulaminu pracy. Taki regulamin winien być uzgodniony z zakładową organizacją związkową, a gdy jej brak lub gdy nie uda się uzgodnić treści regulaminu z organizacją, wówczas pracodawca ustala regulamin samodzielnie i podaje go do wiadomości pracowników. Wszelkie zmiany regulaminu również powinny być przedstawiane w przyjęty u pracodawcy sposób. Istotne jest, że nie tylko sama treść regulaminu powinna być zgodna z prawem, ale także tryb jego wprowadzenia, który jest regulowany przepisami kodeksu pracy.

Kolejnym aktem jest regulamin wynagradzania. Powinien on zostać wdrożony u pracodawców, którzy zatrudniają co najmniej 50 pracowników nieobjętych zakładowym układem zbiorowym pracy ani ponadzakładowym układem zbiorowym pracy. Ustawodawca ustanawia w tej sytuacji obowiązek utworzenia właśnie regulaminu wynagradzania⁸⁵. Jeśli w organizacji jest zatrudnionych mniej niż 50 pracowników, również nieobjętych układami zbiorowymi pracy, pracodawca może (fakultatywnie) wprowadzić regulamin wynagradzania i w nim określić warunki wynagradzania za pracę. W wypadku mniejszej liczby pracowników występuje fakultatywność⁸⁶, tj. pracodawca ma wybór w zakresie wprowadzenia regulaminu, gdy zatrudnia on co najmniej 20 pracowników, ale mniej niż 50 regulamin wynagradzania może zostać wprowadzony, jeśli zakładowa organizacja związkowa wystąpi z wnioskiem o jego ustalenie.

W przepisie ustawodawca posłużył się zwrotem „pracodawca zatrudniający pracowników, nieobjętych układem zbiorowym pracy”, co oznacza, że nie ma znaczenia liczba zatrudnionych, lecz to, jaka grupa pracowników została objęta postanowieniami układowymi⁸⁷.

⁸⁵ Baran K.W. (red.), *Kodeks pracy. Komentarz*, wyd. IV, 2018.

⁸⁶ *Ibidem*.

⁸⁷ *Ibidem*.

Analizując przepisy dotyczące wprowadzenia regulaminu wynagradzania, można przyjąć, że w stosunku do pracodawców, którzy są zobligowani do jego wprowadzenia, ustawodawca nie przewidział specjalnej sankcji⁸⁸, niemniej z punktu widzenia sytemu zgodności zaleca się, aby taki dokument został wprowadzony. Będzie to także niewątpliwa zaleta dla nowo przyjmowanych pracowników, którzy od początku będą zaznajomieni z transparentnym systemem wynagradzania czy premiovania, co często może być decydującym faktorem przy wyborze nowego pracodawcy.

Kolejną kwestią, którą również warto uregulować w formie polityki, jest używanie sprzętów służbowych, tj. samochodów, telefonów komórkowych i komputerów. Warto pochylić się nad sygnalizowaną wcześniej kwestią używania sprzętów do celów prywatnych i ustanowienia jasnych zasad dotyczących zakresu korzystania z nich przez pracowników do celów niezwiązanych z pracą.

Z innych istotnych zagadnień warto też zwrócić uwagę na zmiany w zakresie przechowywania dokumentacji pracowniczej. Dokumenty pracowników zatrudnianych po 31 grudnia 2018 r. powinny być przez pracodawcę przechowywane przez okres 10 lat. Dla pracowników zatrudnionych po 1 stycznia 1999 r. i przed 31 grudnia 2018 r. okres ten może zostać skrócony z 50 do 10 lat, pod warunkiem złożenia odpowiednich dokumentów do Zakładu Ubezpieczeń Społecznych.

Pojawiły się również zmiany dotyczące akt osobowych, które obecnie składają się nie z 3, a z 4 części. Nowa część D będzie zawierać informacje dotyczące kar porządkowych nakładanych na pracownika. Być może zagadnienie to nie będzie u konkretnego przedsiębiorcy spisane w formie osobnej polityki – choć może być częścią np. polityki obiegu dokumentów

⁸⁸ *Ibidem.*

– to jednak jest istotne, by także na tym polu działanie pracodawcy było zgodne z obowiązującymi przepisami prawa.

4. Polityka zarządzania bezpieczeństwem i higieną pracy

Kolejną ważną kwestią, którą należy poruszyć, jest system zarządzania bezpieczeństwem i higieną pracy (BHP). Służy on ustaleniu polityki i celów pracodawcy, dotyczących bezpieczeństwa i higieny pracy w organizacji, ale przede wszystkim zminimalizowaniu występowania niekorzystnych skutków, czyli np. wypadków czy awarii, a także ustaleniu sposobu postępowania w zakładzie pracy na wypadek ich wystąpienia.

Procedura BHP to jednak nie tylko zapobieganie wypadkom, ale także chorobom zawodowym. Polityka BHP powinna być podpisana przez stosowny organ zarządzający przedsiębiorstwa (np. zarząd w spółce z ograniczoną odpowiedzialnością, określać działania pracodawcy w zakresie BHP oraz zobowiązać do ich realizacji.

Zgodnie z przepisami kodeksu pracy pracodawca ponosi odpowiedzialność za stan bezpieczeństwa i higieny w zakładzie (art. 207 §1 kodeksu pracy). Jest on szczególnie obowiązany, by chronić zdrowie i życie pracowników poprzez zapewnienie higienicznych i bezpiecznych warunków pracy (art. 207 § 2 kodeksu pracy). Obowiązki pracodawcy w zakresie bezpieczeństwa i higieny pracy są:

- bezwarunkowe, czyli obowiązki w tym zakresie mają być spełnione przez pracodawcę niezależnie od spełnienia świadczeń przez pracownika;

- niepodzielne, czyli działania czy zaniechania innych jednostek (np. powiązanych) nie zwalniają pracodawcy od odpowiedzialności za stan BHP w zakładzie;
- podwójnie zakwalifikowane, czyli są powinnościami ze stosunku pracy wobec pracownika, ale także publicznoprawnym wobec państwa;
- realne, czyli są wykonywane w naturze⁸⁹.

Do obowiązków pracodawcy określonych w art. 207 § 2 kodeksu pracy zalicza się m.in. organizowanie pracy w bezpiecznych i higienicznych warunkach, zapewnienie przestrzegania przepisów o BHP, reagowanie na potrzeby w zakresie zapewnienia bezpieczeństwa i higieny pracy oraz dostosowywanie środków podejmowanych w celu doskonalenia istniejącego poziomu ochrony zdrowia czy zapewnienie spójnej polityki zapobiegającej wypadkom przy pracy i chorobom zawodowym⁹⁰.

Warto też wskazać na obowiązek informowania o ryzykach i działaniach oraz wyznaczeniu osoby do udzielania pomocy (art. 207¹ kodeksu pracy). To ostatnie oznacza, że pracodawca ma zapewnić udzielenie pierwszej pomocy osobie poszkodowanej w wypadku, prowadzić dokumentację wypadkową oraz przeprowadzić czynności związane z badaniem wypadku przy pracy⁹¹.

W kontekście powyższego warto odnieść się do obowiązków pracodawcy określonych w Rozporządzeniu Ministra Pracy i Polityki Socjalnej z dnia 26 września 1997 r. w sprawie ogólnych przepisów bezpieczeństwa i higieny pracy. Rozporządzenie to wskazuje na szereg obowiązków, np.:

⁸⁹ Dörre-Kolasa D., *Komentarz do rozporządzenia w sprawie ogólnych przepisów bezpieczeństwa i higieny pracy* [w:] *Akty wykonawcze prawa pracy. Komentarz*, opublikowano: WK 2016.

⁹⁰ Sobczyk A., *Państwo zakładów pracy*, WKP 2017.

⁹¹ *Ibidem*.

- obowiązek utrzymywania pomieszczeń pracy w należytym stanie, czyli w czystości i porządku, zapewnienie ich okresowych remontów i konserwacji (§ 14);
- wymogi dotyczące pomieszczeń pracy i ich wyposażenia – w szczególności w pomieszczeniach pracy pracodawca powinien zapewnić oświetlenie naturalne i sztuczne, odpowiednią temperaturę, wymianę powietrza oraz zabezpieczenie przed wilgocią, niekorzystnymi warunkami cieplnymi i nasłonecznieniem, drganiami oraz innymi czynnikami szkodliwymi dla zdrowia i uciążliwościami (§ 15);
- w pomieszczeniach stałej pracy należy zapewnić oświetlenie dzienne, chyba że jest to niemożliwe lub niewskazane ze względu na technologię produkcji, a na stosowanie oświetlenia wyłącznie elektrycznego pracodawca uzyskał zgodę właściwego państwowego wojewódzkiego inspektora sanitarnego wydaną w porozumieniu z okręgowym inspektorem pracy (§ 25);
- oświetlenie dzienne na poszczególnych stanowiskach pracy powinno być dostosowane do rodzaju wykonywanych prac i wymaganej dokładności, należy zapewnić także oświetlenie elektryczne (§ 26).

W § 28 rozporządzenie wspomina o oświetleniu awaryjnym, wskazując, że w pomieszczeniach i miejscach pracy, w których w razie awarii oświetlenia mogą wystąpić zagrożenia dla życia lub zdrowia pracowników, należy zapewnić oświetlenie awaryjne. Rozporządzenie rozstrzyga też kwestie minimalnej i maksymalnej temperatury (§ 30 i § 36) i wskazuje, że w pomieszczeniach pracy należy zapewnić temperaturę odpowiednią do rodzaju wykonywanej pracy nie niższą niż 14°C (287 K), chyba że względy technologiczne na to nie pozwalają. W pomieszczeniach pracy, w których jest wykonywana lekka praca fizyczna i w pomieszczeniach biurowych temperatura nie może być niższa niż 18°C (291 K). Z kolei maksymalna temperatura nawiewanego powietrza nie powinna przekraczać 70°C (343 K)

przy nawiewie powietrza na wysokości nie mniejszej niż 3,5 m od poziomu podłogi stanowiska pracy i 45°C (318 K) w pozostałych przypadkach.

Jest zalecane, aby pracodawcy w swoich organizacjach stworzyli i wdrożyli takie procedury w zakresie BHP, które będą skuteczne i odpowiednie w danej strukturze, biorąc pod uwagę przedmiot oraz profil działalności pracodawcy. W zakresie skutecznego wdrożenia istotną rolę może odegrać np. określenie zakresów odpowiedzialności, przeprowadzenie identyfikacji obszarów ryzyk w organizacji, tj. obszarów, w których może dojść do wypadku, awarii itd., opisanie w procedurze zasad postępowania np. w sytuacji wypadku przy pracy, wpływanie na motywację pracowników, by chcieli się do tych zasad stosować oraz prowadzenie szkoleń przez wykwalifikowane podmioty, co jednocześnie wyłoży na wywiązywanie się pracodawcy z obowiązku przeprowadzania szkoleń.

W ujęciu międzynarodowych standaryzacji BHP zostały wydane normy, które mogą okazać się pomocne we właściwym wdrożeniu systemu zarządzania bezpieczeństwem i higieną pracy w przedsiębiorstwie. Jeśli procedura jest opracowana na ich podstawie, są wydawane odpowiednie certyfikaty dla przedsiębiorców. W tym miejscu jedynie można zasygnalizować, że chodzi w szczególności o dwie normy BS OHSAS 18001 (ang. *Occupational health and safety management systems – Specification*) i jej polski odpowiednik PN-N 18001 (System Zarządzania Bezpieczeństwem i Higieną pracy według normy: PN-N-18001:2004) oraz nową normę ISO 45001, która w porównaniu do poprzedniej tworzy międzynarodowy standard dostosowany do innych systemów zarządzania określonych przez ISO. Podkreślenia wymaga fakt, że norma ISO 45001:2018 dotyczy nie tylko bezpieczeństwa o charakterze fizycznym, ale także wewnętrznym, bowiem zwraca uwagę na problematykę związaną ze znęcaniem się czy wypaleniem zawodowym.

Nie wchodząc w szczegóły, należy wskazać, że skuteczność działań w zakresie wprowadzenia polityki BHP w organizacji powinna opierać się na kilku filarach, które zostały wyrażone we wskazanych wyżej normach i specyfikacjach. W pierwszej kolejności ważne jest zaangażowanie we wdrażanie zasad BHP nie tylko samych pracowników, ale także osób znajdujących się na szczycie struktury, tak by wszyscy czuli się odpowiedzialni za ich prawidłową implementację. Niezwykle istotną kwestią jest też odpowiednie dostosowanie przedsiębiorstwa do wymogów BHP oraz kontrolowanie działań, które mają służyć realizacji polityki bezpieczeństwa. Dobrym pomysłem jest również dokonywanie okresowych przeglądów wdrożonego systemu pod kątem jego stosowalności⁹².

Wspomniana OHSAS to międzynarodowa specyfikacja systemów zarządzania BHP. Została opracowana w 1999 r., a następnie znowelizowana w 2004 r. i 2007 r.⁹³ System ten może być stosowany w każdej organizacji bez względu na zakres jej działania czy wielkość. Norma ta co prawda nie przewiduje gotowych rozwiązań, lecz prezentuje wytyczne natury ogólnej, np. w jaki sposób wdrożyć, opracować i utrzymać bezpieczeństwo w miejscu pracy. Tym niemniej może okazać się dobrą wskazówką dla wdrażania zasad BHP w organizacji, nawet wtedy, gdy pracodawca nie będzie tworzył procedury wedle wymogów z tych norm, czyli nie będzie certyfikowany⁹⁴. Z drugiej strony posiadanie odpowiedniego certyfikatu ISO nie pozostaje bez wpływu na wiarygodność pracodawcy na rynku pracy od strony czysto ludzkiej – szczególnie dotyczy to branż, w których

⁹² <http://archiwum.ciop.pl/9502>

⁹³ Mrugalska B. *System zarządzania bezpieczeństwem i higieną pracy wg OHSAS 18001:2007 w: Projektowanie systemów zarządzania jakością*, red. M. Jasiulewicz-Kaczmarek, A. Misztal, B. Mrugalska, wyd. Politechniki Poznańskiej, Poznań 2011 w: Mrugalska B., Sławińska M., *Zeszyty naukowe Politechniki Poznańskiej*, Nr 63, 2014.

⁹⁴ Zeng S.X., Shi J.J., Lou G.X., *A synergetic model for implementing an integrated management system: An empirical study in China*, *Journal of Cleaner Production*, 2007 w: Mrugalska B., Sławińska M., *Zeszyty naukowe Politechniki Poznańskiej*, Nr 63, 2014.

ma miejsce wiele wypadków i awarii – ale także może mieć znaczenie procesowe. Niemniej bez względu na to, czy pracodawca zdecyduje się na wdrożenie procedur samodzielnie na podstawie przepisów prawa i nałożone na niego prawem obowiązki, czy też zgodnych z ISO, i tak zawsze można skorzystać z opisanych w tej normie wytycznych, jako swego rodzaju drogowskazu dla stworzenia skutecznej polityki BHP w organizacji.

Rozpoczęcie tworzenia procedury czy polityki BHP w organizacji – bez względu na to, czy ma być ona certyfikowana, czy też nie – należy rozpocząć od wewnętrznego audytu mającego na celu sprawdzenie obszarów ryzyk, które należy opisać i uregulować. Warto też pochylić się nad odpowiednim przeszkoleniem pracowników. Należy sprawdzić, czy istnieją jakieś wymogi branżowe, np. w ramach grupy kapitałowej, które również powinny być w takiej procedurze ujęte i wzięte pod uwagę przy jej tworzeniu. W przedsiębiorstwach np. produkcyjnych warto rozważyć, czy nie byłoby wskazane dokonanie oceny ryzyka zawodowego na poszczególnych stanowiskach pracy.

Opracowując procedury, trzeba pamiętać, by nie były one bezrefleksyjnym czy to przepisywaniem normy czy też procedury, która funkcjonuje w spółce-matce czy innych spółkach-córkach grupy kapitałowej, do której należy pracodawca, lecz były przystające do realiów w organizacji. Powinny być pisane przystępnym i zrozumiałym językiem. Warto też pamiętać, że w niektórych organizacjach będzie wskazane stworzenie kompleksowego systemu zarządzania bezpieczeństwem i higieną pracy, tj. obejmującego politykę BHP, cele BHP, odwołania do dokumentów wewnętrznych organizacji z zakresu BHP itd.⁹⁵

⁹⁵ Mrugalska B., Sławińska M., Zeszyty naukowe Politechniki Poznańskiej, Nr 63, 2014.

Pochylając się nad zaletami wprowadzenia polityki BHP należy wymienić optymalizację w zarządzaniu ryzykiem związanym z wypadkami przy pracy (zmniejszenie liczby wypadków), działania prewencyjne w tym zakresie, zmniejszenie liczby zachorowań na choroby zawodowe, zmniejszenie nieobecności w pracy na skutek choroby, a co za tym idzie – zwiększenie wydajności i poprawa jakości pracy. Brak usystematyzowanej procedury szczególnie u tych pracodawców, u których istnieje duże ryzyko wystąpienia wypadku przy pracy czy poważnej awarii, może skutkować zniszczeniem jego reputacji, utratą przychodów ze względu na nieobecność pracownika czy wysokie koszty procesów i odszkodowań.

5. Podsumowanie

Podsumowując powyższe rozważania, należy stwierdzić, że wdrożenie compliance w obszarze prawa pracy to nie tylko samo opracowanie procedur w obszarach ryzykownych w organizacji; to przede wszystkim zrozumienie, do czego całość działań z tego zakresu ma służyć. Innymi słowy – właściwa motywacja poparta zrozumieniem materii zarówno wśród kadry zarządzającej, jak i wśród pracowników, odgrywa tu kluczowe znaczenie. Nie bez znaczenia jest także rola innych działów – w przypadku prawa pracy będzie to przede wszystkim dział HR – które również mogą pomóc w zarządzaniu i minimalizowaniu ryzyka, oraz polityka szkoleniowa.

W prawie pracy właściwa motywacja i uświadomienie sobie celu podejmowanych działań z zakresu zarządzania zgodnością jest szczególnie doniosłe, gdyż rozważane zagadnienia dotyczą, często w sposób bezpośredni, dużej grupy pracowników – ich życia, zdrowia czy danych wrażliwych, które przekazują przy zawieraniu umowy o pracę. Te aspekty

131

zasługują na sprawną i kompleksową ochronę na najwyższym z możliwych poziomów staranności. W tym kontekście istotną rolę odgrywa także dobrze funkcjonujący proces monitorowania zgodności z regulacjami zewnętrznymi i wewnętrznymi, kontrola wszelkich zmian i nowości mających znaczenia dla pracodawcy.

O Autorach

Joanna Jurasz – radca prawny, Associate Partner i kierownik zespołu ds. compliance w Rödl & Partner. Specjalizuje się w doradztwie transakcyjnym, posiada doświadczenie w zakresie obsługi prawnej procesów restrukturyzacji grup kapitałowych oraz nabywania i zbywania przedsiębiorstw. Przeprowadza audyty i przygotowuje przedsiębiorców do wdrożenia polityki compliance. Ma na koncie liczne badania *due diligence*, przeglądy prawne, jest autorką fachowych publikacji. Doradza w języku angielskim i niemieckim w poznańskim biurze Rödl & Partner. Absolwentka prawa oraz międzynarodowych stosunków gospodarczych i politycznych na Wydziale Prawa i Administracji Uniwersytetu im. Adama Mickiewicza w Poznaniu.

Barbara Kaczała – radca prawny i Senior Associate w Rödl & Partner we Wrocławiu. Specjalizuje się w prawie handlowym i korporacyjnym oraz postępowaniach cywilnych. Posiada doświadczenie w projektach z zakresu compliance oraz badaniach *due diligence*. Doradza międzynarodowym przedsiębiorstwom oraz podmiotom prowadzącym działalność w Specjalnych Strefach Ekonomicznych. Autorka licznych publikacji. Władza językiem niemieckim i angielskim. Absolwentka Wydziału Prawa, Administracji i Ekonomii oraz Szkoły Prawa Niemieckiego Uniwersytetu Wrocławskiego oraz studiów podyplomowych z zakresu obrotu nieruchomościami na Uczelni Łazarskiego w Warszawie.

Kludia Kamińska-Kiempa, LL.M. – radca prawny w krakowskim biurze Rödl & Partner. Jej główne obszary praktyki to prawo pracy, postępowania cywilne oraz ochrona danych osobowych. Posiada doświadczenie w zakresie badań *due diligence* i *legal compliance*. Jest specjalistką

w zakresie prawa niemieckiego oraz autorką licznych publikacji. Klientom doradza w języku niemieckim, angielskim i hiszpańskim. Ukończyła prawo i filologię germańską z językiem angielskim oraz Szkołę Prawa Niemieckiego i Szkołę Prawa Austriackiego na Uniwersytecie Jagiellońskim oraz studia LLM na Uniwersytecie Ruprechta i Karola w Heidelbergu.

Łukasz Napiórkowski – starszy prawnik w Rödl & Partner w Warszawie, aplikant adwokacki. Specjalista w zakresie compliance, prawa handlowego i korporacyjnego oraz obsługi przedsiębiorców w obszarze szeroko rozumianego prawa podatkowego. Posiada doświadczenie w realizacji projektów na rzecz podmiotów polskich oraz zagranicznych. Jest autorem licznych publikacji. Władza językiem niemieckim, angielskim i francuskim. Absolwent Wydziału Prawa oraz Wydziału Zarządzania Akademii Leona Koźmińskiego w Warszawie.

Wojciech Paryś – radca prawny, Senior Associate w poznańskim biurze Rödl & Partner. Specjalista w zakresie doradztwa transakcyjnego, M&A oraz compliance. Na co dzień wspiera przedsiębiorstwa inwestujące i reorganizujące się. Autor artykułów fachowych i popularyzatorskich o tematyce prawnej. Doradza w języku angielskim i niemieckim. Absolwent prawa na Uniwersytecie im. Adama Mickiewicza w Poznaniu.

O Enterprise Europe Network

Sieć Enterprise Europe Network funkcjonuje od 1 stycznia 2008 r. Została powołana w ramach Programu Ramowego na rzecz Konkurencji i Innowacji (CIP), a w perspektywie finansowej Unii Europejskiej na lata 2014–2020 funkcjonuje w ramach Programu na rzecz konkurencyjności przedsiębiorstw oraz małych i średnich przedsiębiorstw (COSME) oraz Horyzont 2020. Sieć oferuje małym i średnim przedsiębiorstwom (MŚP) kompleksowe usługi, które mają im pomóc w pełni rozwinąć ich potencjał i zdolności innowacyjne oraz wesprzeć w pozyskaniu nowych partnerów biznesowych. Enterprise Europe Network jest także pośrednikiem umożliwiającym instytucjom Unii Europejskiej pełniejszą orientację w potrzebach małych i średnich przedsiębiorstw.

Na całym świecie działa około 600 ośrodków Enterprise Europe Network oferujących bezpłatne wsparcie dla przedsiębiorców w postaci kompleksowych usług informacyjnych, szkoleń i doradztwa z zakresu prawa i polityk Unii Europejskiej, prowadzenia działalności gospodarczej w Polsce i za granicą, zamówień publicznych, ochrony danych osobowych, udziału w programach ramowych UE itd.

Ośrodki Enterprise Europe Network są afiliowane przy rozmaitych organizacjach wspierających rozwój gospodarczy, takich jak izby przemysłowo-handlowe, agencje rozwoju regionalnego czy centra wspierania przedsiębiorczości. Źródłem finansowania działalności ośrodków Sieci są środki unijne oraz fundusze pochodzące z budżetu państwa.

135

To największa na świecie sieć wspierająca MŚP w internacjonalizacji. Ponad 60 państw, 600 organizacji, 3000 ekspertów.

Powiązanie międzynarodowego doświadczenia ze znajomością lokalnych rynków. 30 ośrodków w Polsce, co najmniej 1 w każdym województwie, współpraca regionalnych ekspertów z ogólnopolską siecią wspierającą MŚP.

Wsparcie w rozwoju biznesu dzięki zindywidualizowanej pomocy, dostępowi do finansowania i nowym partnerom biznesowym.

Zasada „zawsze właściwych drzwi”, która w praktyce oznacza nieodsyłanie przedsiębiorcy bez udzielenia mu niezbędnych informacji.



Polska Agencja Rozwoju Przedsiębiorczości (PARP) jest agencją rządową, która została powołana w 2000 r. do wspierania rozwoju mikro, małych i średnich przedsiębiorstw. Przez 18 lat działalności Agencja wypracowała wiele form wsparcia, które obejmują finansowanie przedsiębiorstw, usługi rozwojowe, działalność edukacyjną i informacyjną oraz działania na rzecz budowy kultury przedsiębiorczości i innowacyjności w Polsce.

Obszary działalności PARP rozwijają się wraz z rozwojem gospodarczym i wyłanianiem się nowych trendów w przedsiębiorczości i innowacyjności. Tym samym PARP na przestrzeni lat stała się prekursorką w tworzeniu wielu nowych obszarów wsparcia i opracowywaniu zróżnicowanych sposobów udzielania pomocy (finansowanie, edukacja, promocja). Stymulowaniu przedsiębiorczości, innowacyjności i konkurencyjności polskich przedsiębiorców służą nowe instrumenty perspektywy finansowej Unii Europejskiej 2014–2020. PARP jest zaangażowana w realizację trzech programów operacyjnych współfinansowanych ze środków europejskich: Inteligentny Rozwój, Polska Wschodnia, Wiedza Edukacja Rozwój.

Aktywność PARP koncentruje się na pięciu obszarach:

- rozwoju przedsiębiorstw i przedsiębiorczości, przez wspieranie rozwoju nowych pomysłów i modeli biznesowych,
- innowacyjności przedsiębiorstw, przez inicjowanie i kompleksowe wspieranie aktywności przedsiębiorstw w tym obszarze,
- ekspansji międzynarodowej przedsiębiorstw, przez wsparcie przedsiębiorców sektora MSP we wchodzeniu na zagraniczne rynki,
- współpracy wśród przedsiębiorstw i otoczenia biznesu, a więc wsparciu budowania powiązań między nimi,
- tworzenia przyjaznej i innowacyjnej administracji, przez pomoc w kreowaniu polityki innowacyjnej państwa oraz rozwijanie i promowanie takich powiązań w sektorze publicznym.



Polska Agencja Rozwoju Przedsiębiorczości

ul. Pańska 81/83

00-834 Warszawa

telefon: 22 432 80 80

e-mail: biuro@parp.gov.pl

Informatorium PARP

telefon: 0 801 332 202