Whistleblowing - dobre praktyki etycznego biznesu

DZP
więcej niż prawo

PRZY WSPARCIU:

Global Compact
Network Poland

Network Poland

Whistleblowing
- dobre praktyki etycznego biznesu

Autorem raportu jest Kancelaria Domański Zakrzewski Palinka sp.k. przy wsparciu United Nations Global Comact Network Poland z zaangażowaniem przedstawicieli biznesu, strony publicznej, organizacji społecznych i ekspertów ds. whistleblowingu, prawa pracy, ochrony danych osobowych i compliance.

DZP
więcej niż prawo

PRZY WSPARCIU:

Global Compact
Network Poland

Niniejszy raport został przygotowany w oparciu o wiedzę ekspercką autorów raportu, publicznie dostępne źródła prawa, i dane statystyczne, doświadczenia praktyczne uczestników sesji dialogowych oraz wyniki badania rynku prowadzonego przez DZP w 2021 roku.

Autorzy prowadzili prace niezależne, opisując zjawiska oraz opracowując rekomendacje bazujące na danych i materiałach źródłowych, których prawdziwości i kompletności nie weryfikowali. W związku z tym autorzy nie odpowiadają za nie i nie udzielają gwarancji w zakresie poprawności i kompletności niniejszego Raportu.

Żaden z Autorów niniejszego Raportu w jakichkolwiek sposób nie może być odpowiedzialny za wykorzystanie informacji w nim zawartych bez wiedzy i zgody. Autorzy nie ponoszą żadnej odpowiedzialności za czyny i konsekwencje ponoszone przez osoby trzecie ani żadne decyzje podjęte lub nie na podstawie niniejszego Raportu.

Opinie przedstawione w publikacji przez autorów tekstów odzwierciedlają indywidualne poglądy.
Zdjęcia oraz grafiki pochodzą z zasobów autorów tekstów bądź publicznych źródeł.

Spis treści

Przedmowa

Powszechna Deklaracja Praw Człowieka, oraz uznane międzynarodowo standardy pracy i zakazy dyskryminacji, na których straży stoi Organizacja Narodów Zjednoczonych, ma swoją konsekwencję w uregulowaniach prawnych, które chronią sygnalistów. Najlepszym tego przykładem jest Dyrektywa Parlamentu Europejskiego i Rady z dnia 23 października 2019 roku w sprawie ochrony osób zgłaszających naruszenia prawa Unii, wprowadzająca powszechny obowiązek zapewnienia ochrony sygnalistom i będąca pierwszym unijnym aktem prawnym, który kompleksowo ujmuje tę tematykę. Mimo że dotychczas jedynie niektóre podmioty działające w określonych branżach podlegały prawnemu obowiązkowi stworzenia wewnętrznych kanałów nieprawidłowości, to jednak wiele firm wprowadziło unormowania wewnętrzne dotyczące ochrony sygnalistów kierując się przy tym potrzebą spełnienia i promowania najwyższych etycznych standardów.

Cykl sesji dialogowych współorganizowanych przez United Nations Global Compact Network Poland oraz kancelarię Domański Zakrzewski Palinka oraz wieńczący ten cykl raport, stały się forum do ukazania funkcjonujących praktyk. Jednocześnie dyskusja odbywała się w szerokim gronie zarówno biznesu, który wdrożył i przetestował już rozwiązania whistleblowingowe i mógł podzielić się wypracowanymi dobrymi praktykami w tym zakresie, przedstawicieli administracji państwowej, której ekspercki głos w omawianych tematach poszerzył perspektywę spojrzenia na wyzwania z jakimi wiąże się wdrożenie rozwiązań whistleblowingowych, a także przedstawicieli organizacji pozarządowych zajmujących się walką z dyskryminacją. Zasady etyczne związane z ochroną sygnalistów dyskutowane były w oparciu o polityki Organizacji Narodów Zjednoczonych, ze szczególnym uwzględnieniem Konwencji Narodów Zjednoczonych przeciw korupcji oraz Wytycznych ONZ dotyczących biznesu i praw człowieka (The UN Guiding Principles on Business and Human Rights).

Misją stojącą u podstawy tworzenia cyklu sesji dialogowych oraz raportu była potrzeba omówienia możliwie wielu wątków związanych z ochroną sygnalistów i pokazania jak funkcjonowali oni dotychczas w polskim środowisku biznesowym niejednokrotnie przyczyniając się do wczesnego wykrycia nieprawidłowości mających miejsce w organizacjach, minimalizując tym samym związane z nieprawidłowościami straty i wnosząc do firm wartość dodaną. Chcielibyśmy, aby nasz raport stał się przede wszystkim benchmarkiem najlepszych rozwiązań dotyczących ochrony sygnalistów, który może wspomóc firmy stojące przed wyzwaniem zaimplementowania tych rozwiązań w ramach swoich uregulowań wewnętrznych. Jednocześnie kompleksowo omawiając tematykę sygnalistów oraz ich zgłoszeń, mamy nadzieję, że w sposób jasny i klarowny wybrzmiał z tej dyskusji fakt jak dużą rolę odgrywają sygnaliści w usprawnieniu procesów funkcjonujących w ich firmach i że działania, które podejmują wpływają jednoznacznie pozytywnie na interes publiczny.

Dr Anna Partyka-Opiela
Partner,
Domański Zakrzewski Palinka sp. k.

Kamil Wyszkowski
Przedstawiciel i Dyrektor Wykonawczy
UN Global Compact Network Poland

RAPORT

1. O RAPORCIE

17 grudnia mija termin implementacji Dyrektywy Parlamentu Europejskiego i Rady z dnia 23 października 2019 roku w sprawie ochrony osób zgłaszających naruszenia prawa Unii (dalej: Dyrektywa) do krajowego porządku prawnego, a polska ustawa implementująca jest obecnie na etapie projektowania. Pomimo, że obowiązek posiadania systemu whistleblowingowego był dotychczas w prawie polskim uregulowany fragmentarycznie, przedsiębiorcy dostrzegali korzyści płynące z zapewnienia sygnalistom ram dla bezpiecznego komunikowania naruszeń.

Wspólnie z United Nations Global Compact Network Poland zorganizowaliśmy cykl sesji dialogowych, podczas których omawialiśmy zagadnienia oraz dobre praktyki związane z whistleblowingiem. Na podstawie wypowiedzi ekspertów i przedstawicieli biznesu, badania rynkowego oraz własnych doświadczeń w budowaniu systemów zgłaszania nieprawidłowości opracowaliśmy kompleksowy raport, wyczerpująco opisujący stan rozwiązań whistleblowingowych na polskim rynku oraz zmiany, które czekają sektor prywatny w związku z transpozycją unijnej Dyrektywy. Pomimo faktu, iż polska ustawa jest obecnie w fazie projektu, to poszczególne rozdziały naszego raportu odnoszą się także do rozwiązań zawartych w projekcie ustawy o ochronie osób zgłaszających naruszenia prawa (dalej: projekt ustawy). Poza identyfikacją dobrych praktyk, zdecydowaliśmy się również na zawarcie poprzedzonych pogłębionymi analizami rekomendacji. Celem stojącym u podstawy tworzenia zarówno cyklu sesji dialogowych, jak również raportu, było utworzenie forum do podzielenia się swoimi rozwiązaniami z innymi podmiotami oraz pokazanie, że mimo szczątkowych regulacji prawnych, dobre praktyki dotyczące whistleblowingu już funkcjonują w polskiej przestrzeni biznesowej.

Mamy nadzieję, że raport posłuży jako zbiór wskazówek pomocnych w implementacji Dyrektywy oraz postanowień projektowanej ustawy, jak również jako zestaw najlepszych standardów, którymi będą mogły inspirować i kierować się te podmioty, które dopiero rozpoczynają budowę systemów zgłaszania nieprawidłowości. Wierzymy, że lektura raportu pomoże w kreowaniu własnych systemów w oparciu o najlepsze rynkowe rozwiązania, którymi pochwalić mogą się firmy biorące udział w naszym badaniu.

Jednocześnie celem przygotowania raportu było przedstawienie rekomendacji ustawodawcy, aby łatwiejsze było zrozumienie, jakie rozwiązania sprawdziły się dotychczas w praktyce. Wzięcie pod uwagę perspektywy biznesu, który od lat umożliwia dokonywanie zgłoszeń nieprawidłowości i zapewnia ochronę sygnalistom, mogłoby z pewnością stanowić wartość dodaną dla przygotowywanej ustawy implementującej Dyrektywę. Cykl sesji dialogowych oraz będący ich efektem raport stał się platformą, w której biznes mógł przedstawić swoje oczekiwania i obawy związane z projektowaną ustawą, podzielić się doświadczeniami i trudnościami w obsłudze posiadanych systemów zgłaszania nieprawidłowości i ochrony

sygnalistów oraz relacji wewnętrznych i działań na rzecz kształtowania kultury transparentności w organizacji.

Struktura raportu oparta jest o przedstawienie w każdym rozdziale regulacji prawnych dotyczących danego tematu, dobrych praktyk biznesowych zidentyfikowanych w tym zakresie podczas przeprowadzonego badania ankietowego i sesji dialogowych oraz zakładki „Czego potrzebuje biznes?", w której przedstawiamy kwestie, jakie mogłyby zostać jeszcze wzięte pod uwagę przez ustawodawcę w procesie legislacyjnym. W raporcie prezentujemy wybrane wyniki badań odnoszące się do zakresów tematycznych poszczególnych rozdziałów. Sam projekt ustawy o ochronie osób zgłaszających naruszenia prawa spełnia większość oczekiwań biznesu, z uwagi na fakt, iż w dużej części oparty jest na Dyrektywie, jednak są jeszcze kwestie, które wymagają doprecyzowania lub doregulowania. Wskazujemy te kwestie na końcu każdego rozdziału.

Julia Besz, LL.M
Associate / Zespół Compliance

Jakub Dydak
Associate / Zespół Compliance

2. O SYGNALISTACH, O KORZYŚCIACH I O PROBLEMACH ZWIĄZANYCH Z ICH OCHRONĄ

Kim są sygnaliści?

Zgodnie z treścią art. 4 projektu ustawy, pod pojęciem *zgłaszającego* rozumie się osobę fizyczną, która zgłasza lub ujawnia publicznie informację o naruszeniu prawa uzyskaną w kontekście związanym z pracą. Projekt precyzuje otwarty katalog sygnalistów[1] - może to być:

a. pracownik, także w przypadku, gdy stosunek pracy już ustał,
b. osoba ubiegająca się o zatrudnienie, która uzyskała informację o naruszeniu prawa w procesie rekrutacji lub negocjacji poprzedzających zawarcie umowy,
c. osoba świadcząca pracę na innej podstawie niż stosunek pracy, w tym na podstawie umowy cywilno-prawnej,
d. przedsiębiorca,
e. akcjonariusz lub wspólnik,
f. członek organu osoby prawnej,
g. osoba świadcząca pracę pod nadzorem i kierownictwem wykonawcy, podwykonawcy lub dostawcy, w tym na podstawie umowy cywilnoprawnej,
h. stażysta,
i. wolontariusz.

Co ważne, zgodnie z projektem ustawy, zgłaszający podlega ochronie pod warunkiem, że miał uzasadnione podstawy sądzić, że będąca przedmiotem zgłoszenia lub ujawnienia publicznego informacja o naruszeniu prawa jest prawdziwa w momencie dokonywania zgłoszenia lub ujawnienia publicznego i że informacja taka stanowi informację o naruszeniu prawa. Przepisów projektowanej ustawy nie stosuje się natomiast do zgłaszającego, jeżeli:

a. informacja o naruszeniu prawa została zgłoszona na postawie przepisów odrębnych, w szczególności jako skarga lub zawiadomienie o możliwości popełnienia przestępstwa,
b. naruszenie prawa godzi wyłącznie w prawa zgłaszającego lub zgłoszenie naruszenia prawa następuje wyłącznie w indywidualnym interesie zgłaszającego.

Dla porównania, w art. 5 pkt. 7 Dyrektywy *osoba dokonująca zgłoszenia* oznacza osobę fizyczną, która zgłasza lub ujawnia publicznie informacje na temat naruszeń uzyskane w kontekście związanym z wykonywaną pracą. Dyrektywa precyzuje również dodatkowe warunki ochrony sygnalistów. Pod ochroną Dyrektywy znajdują się osoby dokonujące zgłoszenia, pod warunkiem, że osoby te:

(a) miały uzasadnione podstawy, by sądzić, że będące przedmiotem zgłoszenia informacje na temat naruszeń są prawdziwe w momencie dokonywania zgłoszenia, a zgłoszenie danej informacji podlega ochronie (co jest powszechnie rozumiane jako *dobra wiara sygnalisty*)[2] oraz
(b) dokonały zgłoszenia za pośrednictwem kanału wewnętrznego albo zewnętrznego lub dokonały ujawnienia publicznego zgodnie z art. 15 Dyrektywy.

Zarówno Dyrektywa jak i projektowana ustawa obejmują ochroną wszystkie osoby, które, w dobrej wierze i zgodnie z przepisami prawa, zgłaszają nieprawidłowości objęte zakresem Dyrektywy i projektowanej ustawy zaobserwowane w ich środowisku zawodowym, niezależnie od wybranego rodzaju kanału dokonywania zgłoszeń. Przez *kontekst związany z pracą*, o którym wspomina zarówno Dyrektywa jak i projekt ustawy, rozumieć należy przyszłe lub obecne działania związane z pracą (bez względu na podstawę stosunku), niezależnie od ich charakteru i sektora, w związku z którymi sygnalista uzyskał informacje o nieprawidłowościach, a ich ujawnienie może spowodować podjęcie wobec niego działań odwetowych.

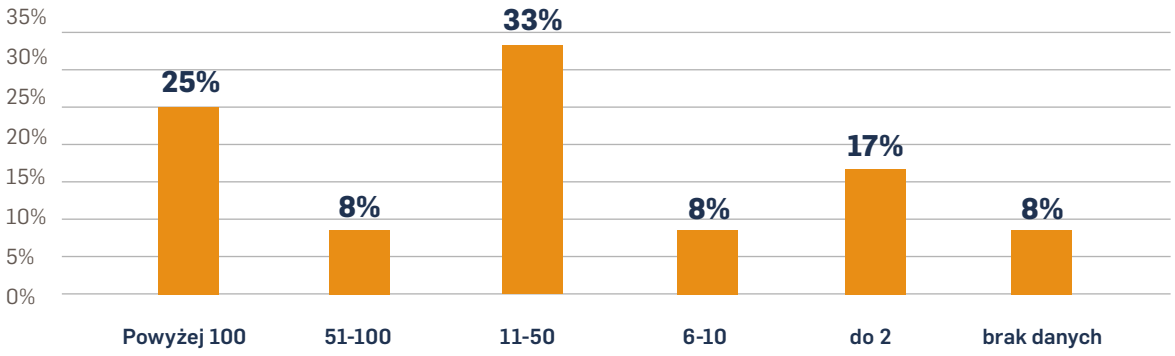
Jak postrzegani są sygnaliści?

W świadomości społecznej sygnaliści nie są jednak powszechnie uważani za osoby, które należy chronić. Stosunek wiekszości społeczeństwa do Sygnalistów jest często bardzo negatywny. Jak wynika z badania postrzegania sygnalistów w Polsce, przeprowadzonego przez Fundację Batorego w 2019 r., aż 35% potencjalnych sygnalistów obawia się, że zostaną uznani za donosiciela, a 18% z nich uważa, że zgłaszanie nieprawidłowości wiąże się z trudnościami. W realiach polskich jest to o tyle poważny problem, że budzi dodatkowo skojarzenia związane z funkcjonowaniem w poprzednim ustroju politycznym. Jest to jednak błędne skojarzenie, ponieważ liczba dokonywanych zgłoszeń w polskich przedsiębiorstwach jest mimo wszystko wysoka, a wskazywane informacje iden-

1 Na potrzeby raportu, pisząc o osobie zgłaszającej naruszenia, używamy pojęcia sygnalista, które oznacza osobę zgłaszającą naruszenia prawa krajowego i unijnego oraz inne nieprawidłowości, której przysługuje ochrona na gruncie zarówno Dyrektywy jak i projektu ustawy.Pojęcie sygnalisty dotychczas nie zostało zdefiniowaneprawnie, jednak jest szeroko stosowane w biznesie, dlatego regulacja ta jest dodatkowo cenna
2 Wymóg ten powtórzony jest kilka razy w projekcie ustawy zarówno wobec zgłoszenia jak i ujawnienia publicznego

tyfikują realne problemy w organizacjach posiadających systemy zgłaszania. Przewaga ankietowanych w badaniu DZP i UNGC wskazała, że rocznie otrzymuje średnio 11 lub więcej zgłoszeń - 25%, że jest ich więcej niż 100.

Średnia liczba otrzymywanych zgłoszeń dotyczących nieprawidłowości



Sygnalistą, któremu na podstawie regulacji wewnętrznych uczestników badania przysługuje ochrona prawna, jest natomiast osoba, która dokonując zgłoszenia ma na celu dobro i interes organizacji i nie oczekuje korzyści osobistych w zamian za zgłoszenie. Z perspektywy sygnalisty, zgłoszenie nieprawidłowości jest jednak najczęściej działaniem obarczonym znacznym ryzykiem osobistym, stąd potrzeba wysokiego poziomu ochrony takich osób. Sygnalista, który podlega ochronie, dokonując zgłoszenia nieprawidłowości może również kierować się:

– *interesem publicznym*, a więc uwzględniając potrzeby lub korzyści dla całego społeczeństwa lub określonych grup społecznych, zagrożone w związku z wystąpieniem nieprawidłowości,

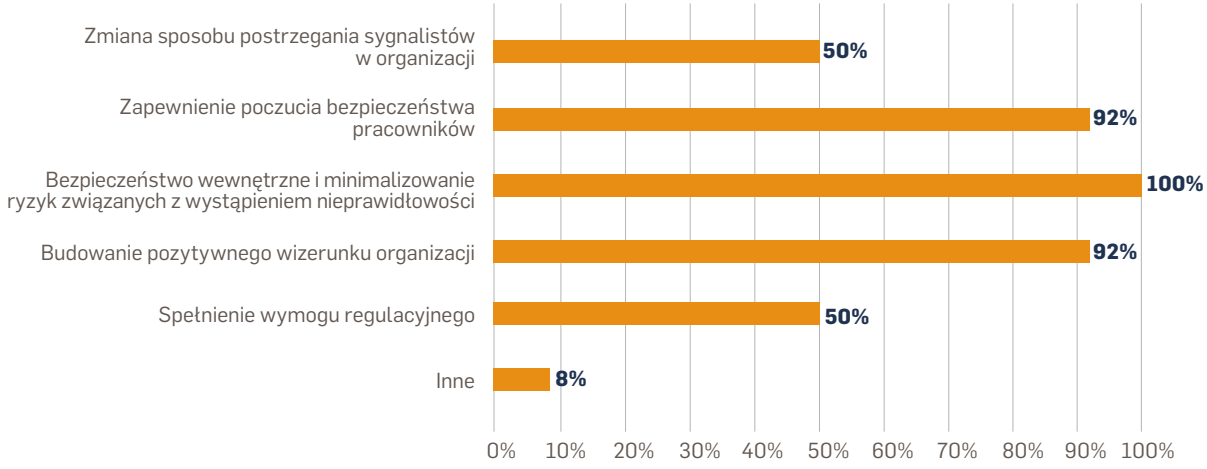
– dobrem swojego miejsca pracy lub

– troską o dochowanie standardów etycznych.

Każdorazowo jednak zgłoszenie musi być dokonane w dobrej wierze. Jak wynika z *Whistleblowing Report* 2019 ponad 50% zgłoszeń dokonywanych przez sygnalistów uważanych jest za przydatne, a jedynie około 9% raportów stanowi nadużycie.

W badaniu przeprowadzonym przez DZP oraz UNGC, 50% ankietowanych wskazało, że zmiana sposobu postrzegania sygnalistów to jeden z celów nadrzędnych realizowanych przez system whistleblowing w ich organizacji.

Nadrzędne cele systemu whistleblowingowego w organizacji



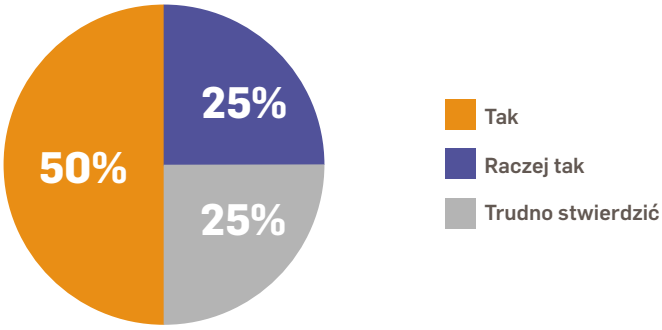
Dlaczego warto chronić sygnalistów?

Zgodnie z zeszłorocznym raportem Association of Certified Fraud Examiners (ACFE) pt. *Report to thevNations: 2020 Global Study on Occupational Fraud and Abuse*[3] aż 32% procent przypadków korupcji na świecie wynika z niewystarczających mechanizmów kontroli wewnętrznej. Branże, które najczęściej padają ofiarą korupcji to m.in. sektor publiczny. Dodatkowo w raporcie ACFE pt. *Fraud in the wake of Covid-19: Benchmarking Report*[4] wskazano, że w następstwie światowej pandemii do maja 2021 r. znacząco wzrośnie ryzyko wystąpienia łapownictwa i korupcji. Z kolei zgodnie z najnowszym raportem CBA dotyczącym zwalczania przestępczości korupcyjnej w Polsce, w 2018 r. zarejestrowano 32 309 przestępstw korupcyjnych, w związku z którymi podejrzanych o przestępstwa korupcyjne było 2 220 osób, a prawomocnie skazano aż 2 046 osób[5]. Liczby te rosną z roku na rok.

Dodatkowo, badania statystyczne wykazują, że zgłoszenia stanowią jedno z najistotniejszych źródeł wiedzy o nadużyciach wewnątrz organizacji. Z raportu ACFE – Report to the Nations 2020 wynika, że wykrytych w ten sposób zostało 43% naruszeń, podczas gdy druga najskuteczniejsza metoda detekcji nadużyć – audyt wewnętrzny – doprowadziła do wykrycia 15% nieprawidłowości. Z badań wynika również, że zaledwie 1% wszystkich nadużyć wykrywany jest dzięki działaniom organów ścigania. Natomiast straty w takich przypadkach są średnio 8 razy wyższe niż w przypadku wykrycia ich wewnątrz organizacji.

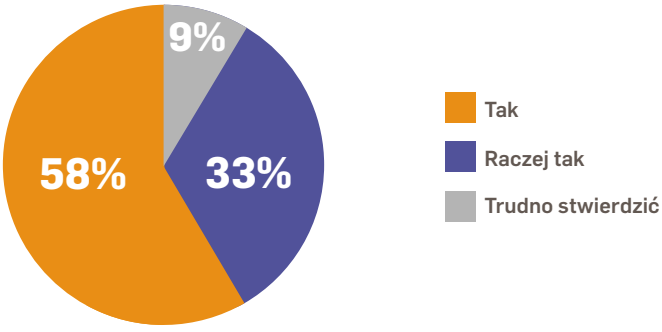
50% ankietowanych w badaniu DZP i UNGC stanowczo wskazało, że posiadanie systemu whistleblowing przyniosło im wymierne korzyści finansowe w zakresie zapobiegania nieprawidłowościom lub ich zwalczania – a 25% skłaniało się ku takiemu stwierdzeniu:

Czy posiadanie systemu whistleblowingowego przyniosło wymierne korzyści finansowe dla organizacji?



Większy odsetek badanych organizacji zadeklarował, że wdrożenie systemu pociągnęło za sobą korzyści o charakterze niefinansowym:

Czy posiadanie systemu whistleblowingowego przyniosło wymierne korzyści w zakresie zapobiegania/zwalczania nieprawidłowości niefinansowych w organizacji?



3 Association of Certified Fraud Examiners, Report to the Nations: 2020 Global Study on Occupational Fraud and Abuse
4 Association of Certified Fraud Examiners, Fraud in the wake of Covid-19: Benchmarking Report
5 Zwalczanie przestępczości korupcyjnej w Polsce 2018 r., Biuro Analiz CBA, Warszawa 2020

Menadżerowie ponad 2 tys. organizacji na całym świecie przypisują średnio 63% wartości rynkowej ich organizacji, jej globalnej reputacji. Z kolei po przebadaniu tysiąca największych organizacji na świecie, stwierdzono, że dobra reputacja organizacji przekłada się na wzrost wartości akcji na giełdzie o 35,3%. Ochrona sygnalistów pozwala pośrednio chronić wizerunek i reputację organizacji. Gdyby nie zgłoszenia wewnętrzne dokonywane przez sygnalistów, informacja o potencjalnych nieprawidłowościach mogłaby dotrzeć do mediów i organów ścigania. Jak się okazuje, ryzyko wizerunkowe związane się z opublikowaniem w mediach informacji o nieprawidłowościach bezpośrednio przekłada się na sytuację finansową organizacji.

Wreszcie – sygnaliści mogą także być ofiarami nieprawidłowości, które zgłaszają. Sygnaliści mogą nie tylko przypadkiem dowiedzieć się o nieprawidłowościach wewnętrznych, ale także nie rzadko doświadczają ich na sobie, np. padając ofiarą phishingu lub otrzymując wiadomość e-miał z linkiem aktywującym złośliwe oprogramowanie. W przypadku nieprawidłowości wewnętrznych, dokonanie zgłoszenia jest dla sygnalisty możliwością uchronienia się przed udziałem w przestępstwie lub poniesieniem negatywnych konsekwencji sprzeciwu.

Szczególna sytuacja kobiet sygnalistek

Jak informuje Amnesty International, przemoc wobec kobiet jest zjawiskiem powszechnym - połowa wszystkich kobiet doświadcza molestowania seksualnego w ciągu swojego życia, 40% doświadcza przemocy psychicznej, a 30% - fizycznej. W styczniu 2018 r. The National Woman's Law Center z siedzibą w Waszyngtonie otworzyła fundusz łączący kobiety, które decydują się zgłosić dostrzegane nieprawidłowości na tle dyskryminacyjnym, mobbingowym i w obszarze molestowania oraz prawników, specjalizujących się w obronie sygnalistów. Na podstawie tysięcy zgłoszeń powstał raport zawierający ogólną analizę wniosków o pomoc prawną w związku z molestowaniem seksualnym, które wpłynęły do funduszu między 1 stycznia 2018 r. a 30 kwietnia 2020 r.

Z raportu wynika, że ponad 70% osób, które doświadczyły molestowania seksualnego w miejscu pracy i zdecydowało się zgłosić ten fakt do organizacji, spotkało się z jakąś formą działań odwetowych, w tym ze zwolnieniami, pozwem o zniesławienie lub z odmową awansu. Prawie 40% wszystkich sygnalistek poinformowało również, że doświadczyło w miejscu pracy napaści na tle seksualnym, gwałtu lub innego rodzaju molestowania fizycznego. W raporcie wskazano również, że ponad 60% sygnalistek zwraca się najpierw do swoich pracodawców, aby zgłosić przypadki takiego odwetu, jednak pracodawcy nie podejmują wobec takiej informacji żadnych działań. Uczestnicy projektu DZP i UNGC wskazali, że w ramach wewnętrznych systemów whistleblowing otrzymują zgłoszenia wewnętrzne dotyczące m.in. dyskryminacji, mobbingu, molestowania seksualnego, nękania, agresji, przemocy, zastraszania oraz naruszenia prywatności osobistej, także będących formą odwetu za działanie sygnalisty.

CZEGO POTRZEBUJE BIZNES?

Prawidłowo działający system whistleblowingowy może stanowić istotny element w walce z nieprawidłowościami w miejscu pracy. Wdrażając Dyrektywę, ustawodawca powinien wziąć pod uwagę statystyki dot. poszczególnych zjawisk i nieprawidłowości w polskich organizacjach, w tym szczególną sytuację osób najbardziej narażonych na doświadczenie naruszeń wewnętrznych. Polski ustawodawca powinien uregulować również obowiązek zapobiegania nieprawidłowościom pracowniczym, w szczególności wszelkim formom przemocy, ale także mobbingowi, dyskryminacji i molestowaniu seksualnemu. Przepisy w tym zakresie na poziomie różnych ustaw są w polskich przepisach dość zdawkowe. Ustawodawca decydując się na wyłączenie z katalogu rodzajów naruszeń (indywidualne) kwestie pracownicze, mógłby rozważyć doprecyzowanie zasad prewencji takich nadużyć - w tym szczególnie występujących jako forma odwetu - w innych przepisach.

3. PRAWO POLSKIE A DYREKTYWA

Polskie regulacje a dyrektywa

Na dzień sporządzania raportu – przed wejściem w życie ustawy o ochronie osób zgłaszających naruszenia prawa – regulacja whistleblowingu ma w polskim porządku prawnym charakter rozproszony. Do posiadania systemów zgłaszania nieprawidłowości zobowiązany jest zamknięty katalog podmiotów, a wymóg ten jest uwarunkowany charakterem prowadzonej działalności. Obowiązek ustanowienia kanałów whistleblowingowych przewidują ustawa AML[1], o ofercie publicznej[2] oraz Prawo bankowe[3].

Prawo bankowe stanowi, że banki zobowiązane są do posiadania systemu zarządzania obejmującego procedury anonimowego zgłaszania nadużyć, umożliwiający zasygnalizowanie naruszenia prawa (w szczególności przepisów ustawy), a także standardów etycznych i procedur przyjętych przez dany podmiot. Za odbiór zgłoszeń odpowiadać ma członek zarządu jednostki, a w wyjątkowych przypadkach – rada nadzorcza.

Analogiczne rozwiązanie przyjęto na gruncie ustawy o ofercie publicznej, podkreślając jednak, że zgłaszane mają być przede wszystkim naruszenia przepisów ustawy i unijnego rozporządzenia 2017/1129.

Inaczej, bardziej ściśle, kwestię stworzenia systemu whistleblowingowego uregulowano w ustawie AML. Na podmiotach zobowiązanych spoczywa obowiązek wdrożenia sformalizowanych procedur anonimowego zgłaszania naruszeń przepisów z zakresu przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu. Akt, jako jedyny z przywołanych, wyznacza minimalny zakres treściowy procedur, a także przewiduje ochronę sygnalisty przed działaniami odwetowymi.

Sytuacja zgłaszających nieprawidłowości zmieni się wraz z wejściem w życie ustawy o ochronie osób zgłaszających naruszenia prawa. Systemy whistleblowingowe będą musieli wdrożyć pracodawcy:

- zatrudniający co najmniej 50 pracowników (z odroczeniem terminu wejścia w życie tego obowiązku dla pracodawców zatrudniających poniżej 250 pracowników do 17 grudnia 2023 r.),
- wykonujący działalność w zakresie usług, produktów i rynków finansowych oraz zapobiegania praniu pieniędzy i finansowaniu terroryzmu, bezpieczeństwa transportu i ochrony środowiska - niezależnie od ilości pracowników.

Chronieni będą sygnaliści, którzy uzyskali informacje o nadużyciach w kontekście związanym z pracą.

Na pracodawcach będzie spoczywał obowiązek ustanowienia regulaminu zgłoszeń wewnętrznych regulujący wewnętrzne procedury przyjmowania zgłoszeń i podejmowania działań następczych. Ponadto mogą oni w ramach regulaminu rozszerzyć zakres naruszeń prawa, których zgłoszenie będzie zapewniało status sygnalisty.

Szczegółowa analiza rozwiązań zawartych w Dyrektywie i projekcie ustawy znajduje się w kolejnych rozdziałach niniejszego raportu. Z perspektywy relacji między prawem polskim, a Dyrektywą istotne jest wskazanie, jakie skutki niesie jej implementacja. Kluczowe różnice w stosunku do dotychczas obowiązujących przepisów dot. sygnalistów zawartych w wyżej wymienionych ustawach, to przede wszystkim powszechność obowiązku stworzenia wewnętrznych regulacji (brak ograniczenia branżowego) oraz szeroki zakres przedmiotowy (możliwy do dalszego poszerzania w regulaminach wewnętrznych). Ponadto należy wskazać stworzenie alternatyw dla sygnalisty w postaci możliwości dokonywania zgłoszeń zewnętrznych oraz ujawnienia publicznego. Jest to pierwsza regulacja, która temat reguluje kompleksowo, jednakże obowiązki istniejące dotychczas nie stoją z nią w sprzeczności.

1 Ustawa z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finasowaniu terroryzmu
2 Ustawa z dnia 29 lipca 2005 r. o ofercie publicznej i warunkach wprowadzania instrumentów finansowych do zorganizowanego systemu obrotu oraz o spółkach publicznych
3 Ustawa z dnia 29 sierpnia 1997 r. Prawo bankowe

CZEGO POTRZEBUJE BIZNES?

Pewnego rodzaju wyzwaniem będzie połączenie wymogów obowiązujących już ustaw i nowej ustawy o ochronie sygnalistów. Rozbieżność wymogów wymienionych, obowiązujących już polskich regulacji whistleblowingowych, a tych z projektu ustawy to przede wszystkim kwestia anonimowości. Projekt pozostawia decyzji pracodawców, to czy chcą oni przyjmować zgłoszenia anonimowe. Przepisy AML, prawa bankowego i ustawy o ofercie publicznej wprowadzają obowiązek ustanowienia anonimowych kanałów zgłaszania, z kolei projekt ustawy w duchu Dyrektywy wymaga, aby zagwarantować ochronę tym osobom, które zgłoszą anonimowo, ale później w toku postępowania ich tożsamość zostanie ujawniona. Wprowadzenie uspójnienia lub wzajemnych referencji w tych przepisach może być cenne z pespektywy budowania systemów whistleblowingowych dla adresatów już obowiązujących przepisów.

4. OBOWIĄZEK POSIADANIA SYSTEMU

Po zidentyfikowaniu potrzeby lub prawnego obowiązku posiadania systemu whistleblowing, każda organizacja stoi przed dylematem, jakie rodzaje kanałów powinny zostać wdrożone. Zgodnie z Dyrektywą należy ustanowić kanały zgłaszania, które są niezależne i autonomiczne. Oznacza to, że:

1. zostały zaprojektowane i ustanowione oraz są obsługiwane w sposób zapewniający kompletność, integralność i poufność informacji oraz uniemożliwiający uzyskanie dostępu nieupoważnionym osobom;

2. pozwalają na przechowywanie informacji w sposób trwały (w ramach odpowiedniego rejestru), aby umożliwić prowadzenie dalszego postępowania wyjaśniającego.

Natomiast - co wynika z przedstawionych przepisów projektu ustawy - każda organizacja, na którą został nałożony taki obowiązek, musi umożliwiać dokonywanie zgłoszeń przynajmniej na piśmie lub ustnie. Zgłoszenie ustne może być dokonane telefonicznie lub za pośrednictwem innych systemów komunikacji głosowej oraz na wniosek zgłaszającego za pomocą bezpośredniego spotkania zorganizowanego w terminie 7 dni od dnia otrzymania zgłoszenia.

Jednocześnie należy mieć na względzie, że decyzja dotycząca wyboru konkretnych kanałów to jednak nie tylko kwestia konieczności spełnienia wymogów prawnych w tym zakresie. Ponieważ każdy kanał posiada swoje wady i zalety, które należy wziąć pod uwagę decydując się na jego wdrożenie.

- **Bezpośrednia rozmowa** – możliwość osobistego zgłoszenia nieprawidłowości pozostaje najpopularniejszym wśród organizacji kanałem zgłaszania. Doświadczenia zaangażowanych w projekt UNGC i DZP organizacji pokazują, że to osobiste zgłoszenia są najbardziej wiarygodne. Wymagają od sygnalisty zmierzenia się z problemem „twarzą w twarz", więc tym samym dużej odwagi. Nie każdy sygnalista jest jednak gotowy na podjęcie takiego kroku. Jest to główna wada tego kanału, bo jego skuteczność zależy w dużej mierze od kultury organizacji oraz wewnętrznych relacji w zespołach. Dodatkowo nie we wszystkich organizacjach pracownicy mają łatwy i bezpośredni dostęp do swoich przełożonych czy osób uprawnionych do przyjmowania zgłoszeń (szczególnie gdy jest to daleka w strukturach organizacji pracownikowi osoba, np. z działu HR czy Compliance ulokowana w strukturach korporacyjnych). Dlatego najlepszą praktyką rynkową jest nie tylko umożliwienie zgłaszania nieprawidłowości bezpośrednim przełożonym czy Compliance Officerowi, ale wyznaczanie odpowiednich osób (np. tzw. rzeczników etyki) cieszących się zaufaniem w poszczególnych działach/lokalizacjach organizacji. Odpowiednio szkoląc takie osoby, wiemy, że zachowają się poprawnie w przypadku otrzymania zgłoszenia i będą wiedzieć, w jaki sposób chronić sygnalistę. Osobisty kanał nie zapewnia też anonimowości wymaganej częścią polskich przepisów.

- **Dedykowany adres e-mail** – dedykowany adres e-mail to prawdopodobnie najprostszy sposób na organizację systemu zgłoszeń pisemnych z perspektywy firm. Posiada on też wiele zalet. Jest to sprawdzony i wygodny sposób na dwustronną komunikację z sygnalistą. Umożliwia również załączanie dowodów do wiadomości e-mail. Należy mieć jednak świadomość wad takiego rozwiązania. Po pierwsze, możliwe jest co prawda założenie specjalnej skrzynki pocztowej przez sygnalistę, jednak wciąż nie zapewnia to pełnej anonimowości oraz jest uciążliwe dla potencjalnych zgłaszających. Po drugie, samemu rozwiązaniu brakuje bezpieczeństwa bardziej zaawansowanych platform, ponieważ to dostawca poczty po stronie sygnalisty w pewnym stopniu odpowiada za standard bezpieczeństwa (szczególnie gdy zgłoszenie zawierające sensytywne informacje spływa do nas z poczty innej niż służbowy adres e-mail pracownika). Po trzecie, udostępnienie skrzynki nie wymusza użycia formularza, w związku z czym narażamy się na otrzymywanie niepełnych zgłoszeń, a sami sygnaliści często nie odpowiadają na ewentualne dodatkowe pytania zadane w reakcji firmy na zgłoszenie.

- **Dedykowany formularz online** – formularz eliminuje część wad, które posiada kanał oparty na adresie e-mail. Strukturyzuje on zgłoszenie i wymusza podanie najważniejszych informacji. Umożliwia łatwe zachowanie anonimowości, wciąż będąc prostym sposobem kontaktu dla sygnalisty. Ma jednak wadę w postaci braku łatwej możliwości zachowania dwustronnej komunikacji przy jednoczesnym zachowaniu anonimowości. Wciąż wymaga to najczęściej założenia osobnego adresu e-mail przez sygnalistę, co powiela wcześniej wskazane ryzyka. Należy też pamiętać, że korzystając z zewnętrznych rozwiązań formularzy, polegamy na standardach bezpieczeństwa często niedostosowanych do wrażliwości przekazywanych tymi kanałami informacji.

- **Telefon zaufania** – skuteczność telefonu zaufania zależna jest od zasobów organizacji. Utrzymywanie gorącej linii działającej 24/7 bywa kosztowne, dlatego większość organizacji decyduje się jedynie na wskazanie numeru telefonu do określonej osoby. Wiąże się to z ryzykiem

braku reakcji na telefon z uwagi na inne obowiązki. Nie rozwiązuje tego problemu możliwość nagrania się na pocztę głosową, ponieważ często prowadzi do pozyskania niepełnych informacji. Telefon nie jest to więc rozwiązaniem w pełni niezawodnym. Anonimowość takiego rozwiązania także nie jest pełna. Nawet zastrzegając numer, osoba odbierająca zgłoszenie uzyskuje pewne informacje o sygnaliście takie jak płeć czy charakterystyczne sposoby mówienia np. jąkanie. Niejednokrotnie może umożliwiać to identyfikację sygnalisty mimo braku jego woli. Nie można wykluczyć też możliwości podsłuchania, szczególnie gdy telefon zaskoczy nas w niedogodnym momencie czy niedosłyszenia pewnych treści zgłoszenia. Dodatkowo projekt ustawy w żaden sposób co prawda nie określa, czy możliwe jest nagrywanie rozmowy z sygnalistą w przypadku zgłoszeń wewnętrznych, natomiast - co wynika z przepisów Dyrektywy - możliwe jest nagrywanie prowadzonych rozmów za zgodą sygnalisty. Wydaje się zatem, że udostępnienie takiego kanału zgłaszania to dobry pomysł jako rozwiązania uzupełniające. Umożliwia bezpośredni kontakt z sygnalistą, przy zachowaniu minimum prywatności rozmówcy. Aby jako podstawowy kanał zgłaszania spełniało jednak wszystkie wymagania prawne, wymagałoby to znacznych nakładów technicznych.

- **Dedykowany adres na listy pocztowe** – Zgłoszenia listowne wbrew pozorom cieszą się nieustannie dużą popularnością wśród sygnalistów, szczególnie, gdy pochodzą z zewnątrz organizacji np. od pracowników dostawców/kontrahentów lub byłych pracowników. Organizacje mogą zastanowić się nad stworzeniem specjalnego adresu, na który możliwe będzie wysyłanie poufnej korespondencji, która nie powinna trafiać na główny adres spółki. Listowne zgłoszenia uniemożliwiają jednak kontakt z sygnalistą, mogą być wybrakowane i nie są rozwiązaniem bezpiecznym z perspektywy wielu organizacji. Wymagają też opłacenia przez sygnalistę oraz, z uwagi na naturę poczty, mogą nie trafić do adresata, dlatego zgodnie z najlepszą praktyką rynkową nie powinny być traktowane jako podstawowy kanał zgłoszeń pisemnych.

- **Dedykowana fizyczna skrzynka na terenie zakładu** – jest to rozwiązanie szczególne istotne, gdy w organizacji pracują pracownicy niższego szczebla (np. tzw. *blue collars*). Są to przykładowo pracownicy, którzy pracują wyłącznie na halach produkcyjnych i nie posiadają dostępu do sprzętu służbowego. Umieszczenie fizycznej skrzynki na terenie zakładu umożliwia im bezpieczne i anonimowe zgłaszanie nieprawidłowości. Należy zaznaczyć, że istotne jest umieszczanie skrzynki w miejscach ustronnych, maksymalnie utrudniających podejrzenie czynności wrzucania listu. Stosując takie rozwiązanie musimy jednak pamiętać o konieczności regularnego sprawdzania stanu skrzynek przez zaufane osoby. Miejsce takie nie może być też monitorowane, co jednocześnie naraża organizację na próbę nieautoryzowanego otwarcia takiej skrzynki siłą i braku kontroli nad wykradzionymi danymi.

- **Specjalna platforma IT** – docelowo mają one łączyć zalety wszystkich rozwiązań, ale z drugiej strony, źle zaprojektowane lub wdrożone, mogą posiadać dyskwalifikujące je wady, np. zbyt skomplikowane funkcjonalności lub niedostateczny poziom bezpieczeństwa technicznego. W założeniu jednak dobrze działająca platforma zapewnia pełną anonimowość – również bez możliwości śledzenia po numerze IP i metadanych – jednocześnie zapewniając możliwość utrzymywania kontaktu z sygnalistą, procedowania zgłoszenia i archiwizowania go zgodnie z przepisami na poziomie tego samego narzędzia. Platforma najczęściej proponuje konkretny formularz zgłaszania zbierający minimum niezbędnych do wyjaśnienia sprawy informacji, co też ułatwia zgłoszenie samemu sygnaliście - szczególnie gdy jej obsługa z perspektywy sygnalisty jest intuicyjna. Jedną z największych zalet jaką mają platformy to (przynajmniej częściowe) dbanie o zgodność procesu wyjaśniania nieprawidłowości i archiwizowania zgłoszeń z wymaganiami prawnymi. Dobrze stworzone rozwiązanie IT jest jednocześnie rejestrem zgłoszeń czy przypomina o konieczności udzielenia feedbacku.

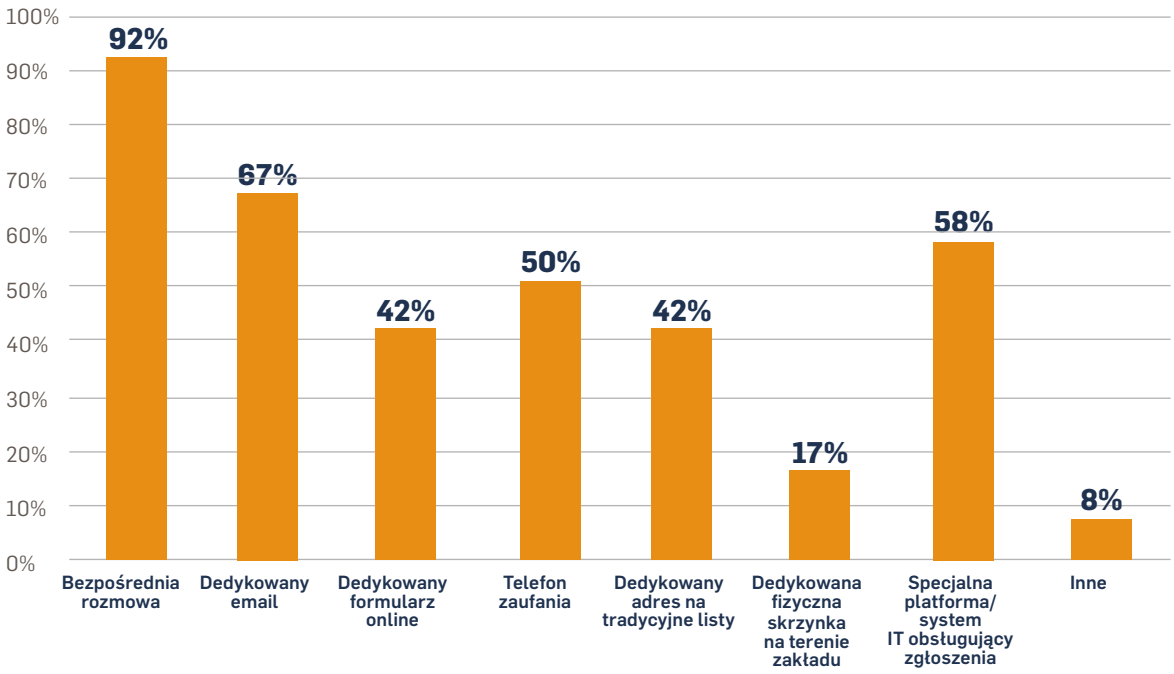
	Zapewnianie anonimowości	Komfort dla sygnalisty	Możliwość utrzymania kontaktu	Bezpieczeństwo informacji	Kompletność zgłoszenia	Możliwość rejestrowania działań naprawczych w związku ze zgłoszeniem	Możliwość archiwizacji zgłoszeń
Bezpośrednia rozmowa	Nie	Mieszane	Tak	Tak	Tak	Nie	Nie
Dedykowany adres e-mail	Mieszane	Tak	Tak	Tak	Nie	Nie	Nie
Dedykowany formularz online	Tak	Tak	Nie	Tak	Tak	Nie	Nie
Telefon zaufania	Mieszane	Mieszane	Mieszane	Mieszane	Mieszane	Nie	Nie
Dedykowany adres na listy pocztowe	Tak	Mieszane	Nie	Mieszane	Nie	Nie	Nie
Dedykowana fizyczna skrzynka na terenie zakładu	Tak	Nie	Nie	Nie	Nie	Nie	Nie
Platforma IT	Tak	Tak	Tak	Tak	Tak	Tak	Tak

Co ciekawe w pytaniu, które z udostępnianych kanałów uczestnicy badania uznają za najbardziej efektywne, nie uzyskano jednolitych odpowiedzi. Część ankietowanych wskazywała na rozmowę bezpośrednią, a część na formularze internetowe, adresy e-mail czy platformy IT. Pokazuje to wątpliwości, jakie posiadają organizacje w zakresie wdrażania kanałów zgłaszania. Z punktu widzenia ustawodawstwa istotne jest zatem dobre opisanie wymagań stawianych takim kanałom, tak żeby niezależnie od wdrożonego rozwiązania, organizacje miały pewność, że są zgodne ze stawianymi przed nimi obowiązkami. Szczególnie ważne może być dostosowanie kanałów do potrzeb konkretnych grup pracowników. Stąd wiele organizacji wdraża lub rozważa uruchomienie więcej niż jednego z nich.

Można także rozważyć outsourcing części procesu systemu zgłaszania do organizacji zewnętrznych. Wtedy kancelaria prawna lub inny zaufany podmiot zewnętrzny odpowiadają za obsługę skrzynki e-mail lub dedykowanej platformy czy odbiór zgłoszeń w dowolnej innej formie od sygnalistów. Niektóre organizacje outsourcują całość działań do takiego podmiotu, co oznacza jego zaangażowanie i wsparcie w procesie wyjaśniania, archiwizowania i prowadzenia całej dokumentacji w związku ze zgłoszeniem. Każdy kanał obsługują wtedy profesjonaliści, więc niewątpliwą zaletą takich rozwiązań jest ekspercka analiza każdego zgłoszenia i oparte na doświadczeniu podejście do sygnalisty. Należy jednak pamiętać, że outsourcując obsługę kanałów, istotna jest przede wszystkim odpowiednia komunikacji między podmiotem zewnętrznym a organizacją. Nie można zapominać, że niemożliwe jest przeprowadzenie postępowania wyjaśniającego bez udziału organizacji, a by efektywnie chronić sygnalistów konieczne są również proaktywne działania osób ze strony osób wewnątrz organizacji. Mimo to zlecanie obsługi zgłoszeń na zewnątrz pozwala istotnie odciążyć zasoby wewnętrzne, a decydują się na to najczęściej firmy, którym zależy na dodatkowym zwiększeniu zaufania do kanałów poprzez pokazanie, że przyjęcia zgłoszenia dokonuje całkowicie obiektywny i niezależny podmiot[1]. Dodatkowo podmioty zewnętrzne zapewniają należyta troskę o ochronę tożsamości sygnalisty, wiedzą, jak wzbudzić jego zaufanie oraz formułują rekomendacje w zakresie postępowania wyjaśniającego i środków naprawczych. Odsuwając częściowo proces obsługi zgłoszeń na wyspecjalizowany podmiot, minimalizujemy też ryzyko strat wizerunkowych i odpowiedzialności osobistej. W przypadku kancelarii prawnych, obsługa zgłoszenia mogą być również objęta tajemnicą adwokacko-radcowską.

1 Projekt ustawy dopuszcza możliwość outsourcingu procesu whistleblowingowego pod warunkiem zawarcia dedykowanej umowy. Nie zwalnia to jednak organizacji z odpowiedzialności za prawidłowe funkcjonowanie systemu

Wdrożone w organizacji kanały zgłaszania nieprawidłowości



CZEGO POTRZEBUJE BIZNES?

Uczestnicy raportu wskazują, że przydatne może być określenie w polskiej ustawie wymagań stawianych podmiotom zewnętrznym świadczących usługi polegające na wspieraniu organizacji w przyjmowaniu zgłoszeń o nieprawidłowości oraz prowadzenia postępowań wyjaśniających. Wymagania te powinny dotyczyć zarówno strony technicznej, w szczególności zapewnienia bezpieczeństwa informacji, ale też prawno-organizacyjnej, tj. w jakim zakresie poszczególne obowiązki muszą być wypełniane przez organizację, a w jakim przez podmiot trzeci. Pomocne byłyby też wskazówki dot. zakresu i formy takiej umowy pomiędzy organizacją, a podmiotem zewnętrznym. Szczególnie, że w wielu przypadkach za taki podmiot zewnętrzny firmy uznają spółkę-matkę w strukturach grup kapitałowych, w których funkcjonują. Tego typu wykonawcze wskazówki mogłyby mieć wydźwięk na poziomie rozporządzeń właściwych ministerstw, a niekoniecznie na poziomie samej ustawy.

5. ODPOWIEDZIALNOŚĆ ZA SYSTEM

Podstawą prawidłowego działania każdego procesu w organizacji jest właściwe przydzielenie odpowiedzialności za jego wdrożenie oraz za nadzór i administrowanie nim. Nieinaczej jest w przypadku procesu zgłaszania i rozpatrywania nieprawidłowości.

Odpowiedzialność za wdrożenie

Proces kompleksowego wdrożenia systemu whistleblowing w organizacji to zadanie nie tylko dla jednej osoby czy nawet działu. W momencie, gdy w życie wchodziły polskie regulacje AML lub ustawa o ofercie publicznej, wiele firm decydowało się na wdrożenie fasadowych rozwiązań whistleblowing, chcąc szybko spełnić nowe wymogi prawne (szczególnie, że na spełnienie ich wymogów nierzadko było bardzo mało czasu). Dopiero z czasem praktyka rynkowa i potrzeby wewnętrzne skłaniały przedsiębiorców do większej formalizacji systemu i urealnienie działań w takim systemie.

Dziś pełne wdrożenie systemu obejmuje m.in. analizę organizacji pod kątem wyboru najbardziej efektywnych kanałów zgłaszania, konsultacje prawne w zakresie spełniania rozsianych po przepisach wymogów prawnych, wyznaczenie osób odpowiedzialnych, usankcjonowanie systemu w procedurach wewnętrznych, organizację szkoleń dla pracowników i osób mających rozpatrywać zgłoszenia, stworzenie odpowiedniego zaplecza technicznego dla kanałów zgłaszania. Oznacza to, że w takie wdrożenie zaangażowana musi być cała organizacja. W tym zakresie liczy się zatem tzw. *tone from the top*. Osoba wdrażająca – najczęściej Compliance Officer, główny prawnik, ale też często inna osoba na stanowisku kierowniczym– powinna mieć udzielone wyraźne wsparcie prezesa/członków zarządu. Tylko w ten sposób jest w stanie pozyskać odpowiednie środki i umocowanie do działania potrzebne do przeprowadzenia wdrożenia i efektywnie skoordynować pracę różnych działów.

Dodatkowo zgodnie z art. 6 ustawy AML, instytucje obowiązane na gruncie ustawy muszą wyznaczyć kadrę kierowniczą wyższego szczebla odpowiedzialną za wykonywanie obowiązków określonych w ustawie. Takim obowiązkiem jest też ustanowienie anonimowych zasad zgłaszania, co dodatkowo podkreśla konieczność udzielania wsparcia we wdrożeniu ze strony najwyższego kierownictwa.

Aktualny projekt ustawy o ochronie osób zgłaszających naruszenia prawa nie zawiera jednak takich przepisów, choć ustanawia dotkliwe sankcje za niewdrożenie systemu whistleblowing lub utrudnianie zgłoszeń, brak ochrony tożsamości sygnalisty i działania odwetowe (w każdym przypadku grzywna lub kara ograniczenia wolności albo pozbawienia wolności do lat 3). Szczególnie przepis karny, który za nieustanowienie wewnętrznej procedury zgłaszania i podejmowania działań następczych (lub zrobienie tego w wadliwy sposób) przewiduje surowe sankcje osobiste, powinien być motywacją dla osób zarządzających przedsiębiorstwem, by właściwie skonstruować swój system i tym samym właściwie wyznaczyć osoby odpowiedzialne za jego wdrożenie, co może wymagać przemyślenia funkcji, ról i uprawnień w ramach systemu.

Odpowiedzialność za administrowanie systemem

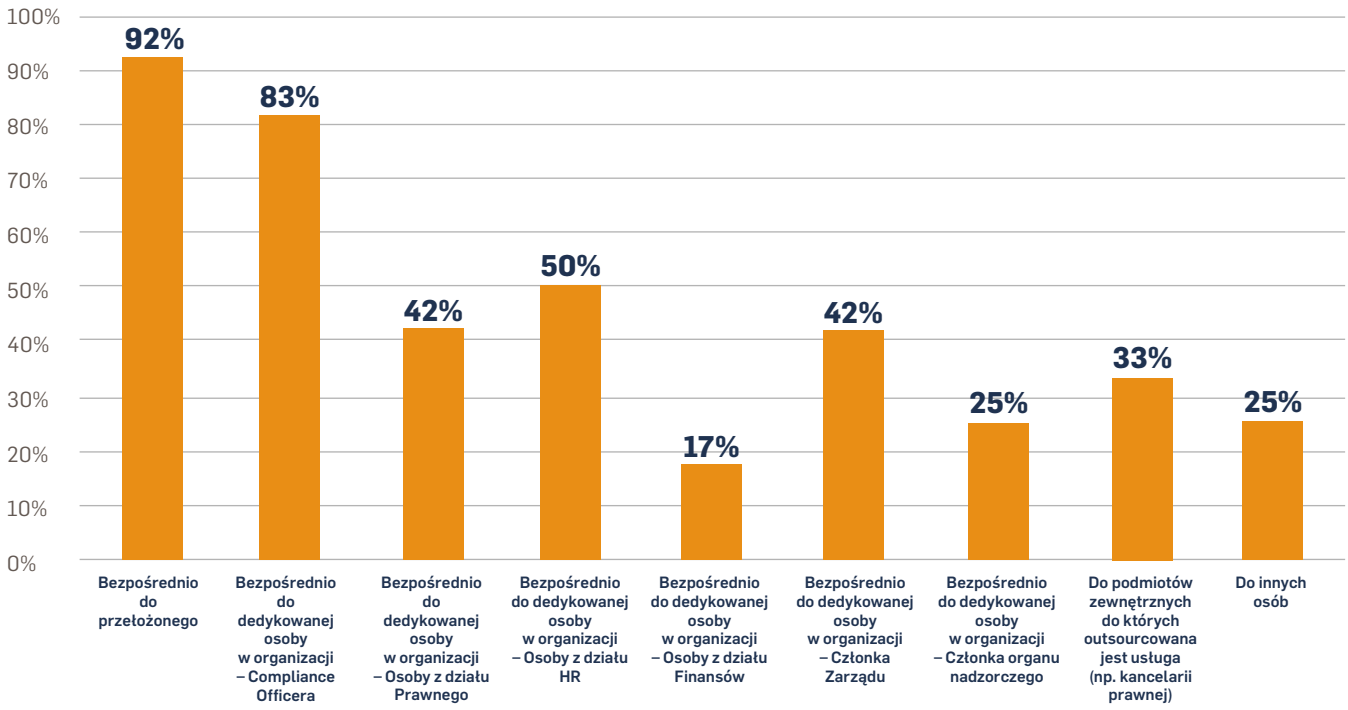
Art. 9 Dyrektywy i 29 ust. 3 projektu ustawy mówi o konieczności wyznaczania bezstronnego podmiotu (rozumianego jako osobę, wydział lub niezależny podmiot zewnętrzny) do podejmowania działań następczych w związku ze zgłoszeniami oraz przyjmowania zgłoszeń.

Natomiast ustawa o AML w art. 53 ustanawia konieczność wyboru osób odbierających zgłoszenia, przy czym wybór ten jest ograniczony do konieczności zapewniania sygnalistom ochrony przed działaniami represyjnymi.

Oznacza to, że akty prawne nie mówią, kto ma odbierać i rozpatrywać zgłoszenia, ale jaki ma być efekt i warunki pracy takich osób.

Badanie przeprowadzone przez DZP i UNGC pokazuje, że do przyjmowania zgłoszeń w organizacjach zobowiązani są najczęściej bezpośredni przełożeni oraz Compliance Officer'owie.

Osoba, do której kierowane są wewnętrzne zgłoszenia nieprawidłowości



Trudny do spełnienia może być szczególnie wymóg bezstronności. Oznaczać to może konieczność angażowania osób z jednej strony podsiadających odpowiednie kompetencje decyzyjne do wyjaśniania nieprawidłowości, ale też z drugiej strony, osób niezależnych od biznesowych aspektów działania organizacji. (tj. podejmujących decyzje niezależnie od pokusy np. wypracowania większego zysku dzięki nieprawidłowości). Jak wskazują uczestnicy badania, w 66% przypadków decyzje co do działań następczych są podejmowane gremialnie – tj. w ramach specjalnie powoływanych komisji. Jest to najlepsza praktyka rynkowa, ponieważ pozwala na zebranie doświadczeń różnych działów i tym samym podjęcie bardziej obiektywnej i tym samym bezstronnej decyzji. Jak pokazuje doświadczenie firm, dobrze do takich komisji angażować w pierwszej kolejności osoby spoza biznesu, tj.: pochodzące z działów compliance, prawnych czy HR. To, jakie osoby powinny rozpatrywać zgłoszenia, jest istotną kwestią mogącą wymagać doprecyzowania przez ustawodawcę.

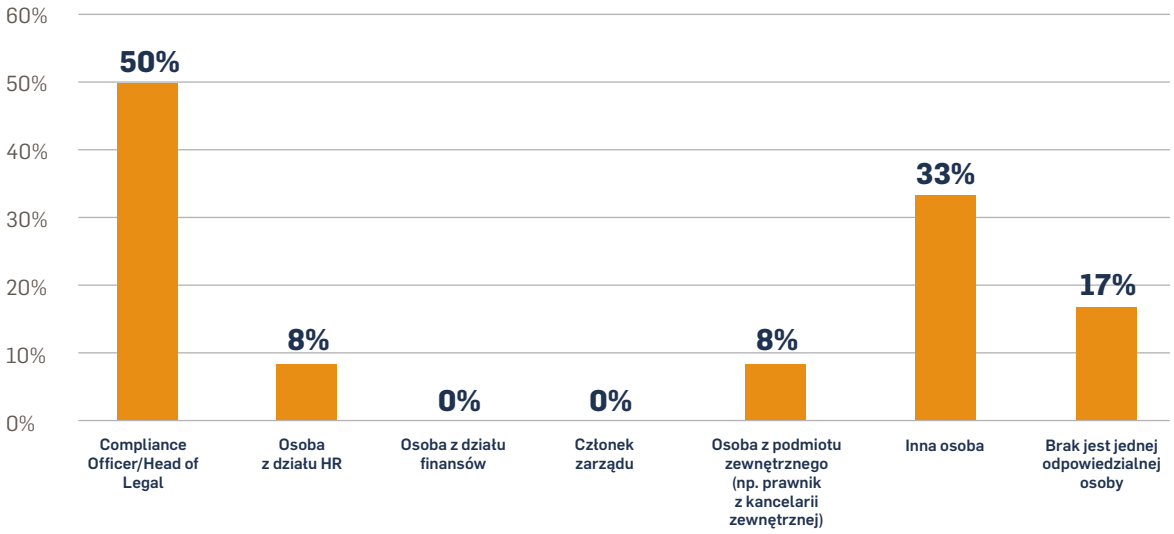
Jak wskazano w poprzednim rozdziale, polski prawodawca w projekcie ustawy wprost dopuszcza też outsourcing administrowania systemu whistleblowing. Procedura zgłoszeń wewnętrznych może bowiem określać „niezależny organizacyjne" od pracodawcy podmiot odpowiedzialny za przyjmowanie zgłoszeń, podejmowanie działań następczych, włączając w to weryfikację zgłoszenia i dalszą komunikację ze zgłaszającym.

Odpowiedzialność za nadzór nad systemem

Przepisy Dyrektywy, polskich ustaw i projektu ustawy nie określają wprost kwestii nadzoru nad systemem, jednak nie ulega wątpliwości, że konieczne jest ustanowienie osoby odpowiedzialnej za taki nadzór. Osoba taka nie tylko powinna czuwać nad jego prawidłowym funkcjonowaniem, ale też dbać by system był aktualny, monitorować przepisy w zakresie whistleblowingu i doskonalić system w miarę zmieniających się okoliczności prawnych czy biznesowych, w których funkcjonuje organizacja. Jak wskazują firmy, rolę taką przyjmuje najczęściej Compliance Officer. Najlepszą praktyką rynkową jest przy tym takie umieszczenie Compliance Officera w strukturze organizacji, by był on zależny wyłącznie od prezesa zarządu (alternatywnie może raportować do Rady Nadzorczej), ponieważ zapewniamy wtedy jego pełną bezstronność, o której mówi projekt ustawy i stan-

dardy compliance. Zgodnie z najlepszą praktyką rynkową, osoba taka powinna też w cyklach rocznych przedstawiać sprawozdanie zarządowi z działania systemu whistleblowing, co umożliwia ujawnienie największych problemów, z jakimi mierzy się organizacja (przydatne w procesie cyklicznej identyfikacji i oceny ryzyk braku zgodności) oraz dać impuls do wprowadzania systemowych rozwiązań niwelujących te problemy.

Osoba sprawująca nadzór w organizacji nad systemem zgłaszania nieprawidłowości



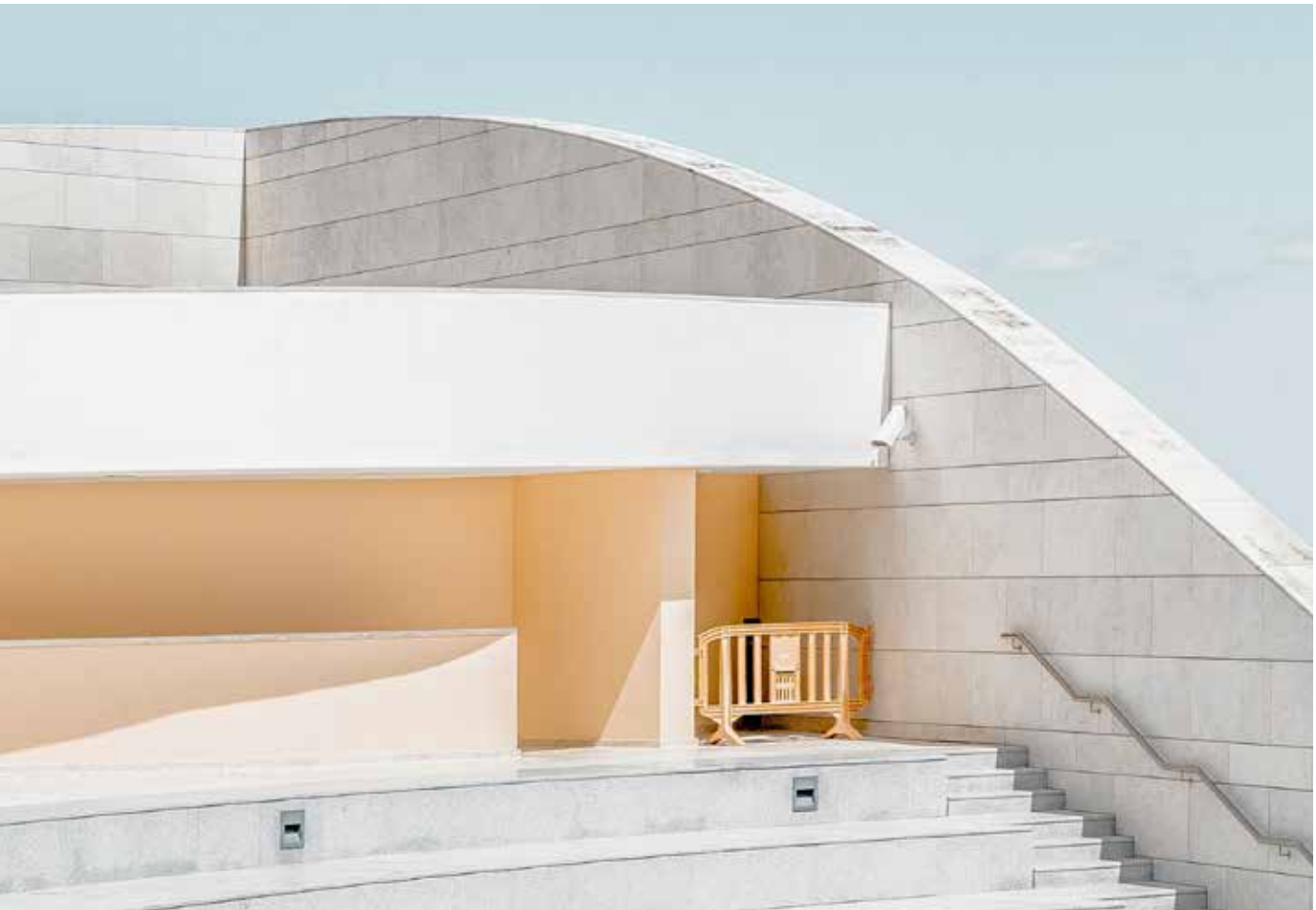
Zobowiązanie do poufności

Ponieważ Dyrektywa jak i polskie ustawy największy nacisk kładzie na zapewnienie poufności i bezpieczeństwa sygnalistom, istotne jest też zadbanie o te kwestie również przy delegowaniu zadań innym osobom w organizacji. Gdy postępowanie wyjaśniające jest skomplikowane, nieuchronnie zaczyna angażować coraz więcej innych osób w organizacji. Istotne jest zatem zadbanie by mimo zwiększania się liczby osób mających wiedzę o nieprawidłowości, dbać o poufność i bezpieczeństwo sygnalisty i wrażliwych informacji. Zgodnie z najlepszą praktyką rynkową, w przypadku pracowników, którzy nie są członkami komisji wyjaśniających lub nie są odpowiednio przeszkoleni, firmy mogą stosować obowiązek podpisywania zobowiązań do poufności, określające również konsekwencje osobiste działania z narażeniem sygnalisty. Należy też zawsze rozważyć, na ile informacja o szczegółach zgłoszenia jest potrzebna danej osobie i na ile dane zadanie może być wykonane bez takiej wiedzy.

Kwestie te są również szeroko poruszane w projekcie ustawy, który w art. 30 ust. 2 wyraźnie stanowi, że do przyjmowania i weryfikacji zgłoszeń, podejmowania działań następczych oraz przetwarzania danych osobowych osób, mogą być dopuszczone wyłącznie osoby posiadające pisemne upoważnienie pracodawcy. Dobrą praktyką rynkową byłby dołączanie do takiego upoważnienia pisemnych zobowiązań do poufności, co pozwoli wykazywać dodatkową należytą staranność w zakresie dbania o ochronę tożsamości sygnalisty. Takie działanie ma to przede wszystkim charakter uświadamiający.

Odpowiedzialność pracownicza

Odpowiedzialność za prawidłowe funkcjonowanie systemu compliance powinna ciążyć nie tylko na osobach rozpatrujących zgłoszenie i kadrze kierowniczej, ale też na pracownikach niższych szczebli. Jeżeli odpowiednio stworzymy struktury systemu, zapewnimy bezpieczeństwo sygnalistom i odpowiednio zakomunikujemy zasady funkcjonowania systemu na dedykowanych szkoleniach, możemy oczekiwać współpracy w zakresie zgłaszania nadużyć ze strony pracowników. Część organizacji decyduje się na formalne zobowiązanie pracowników



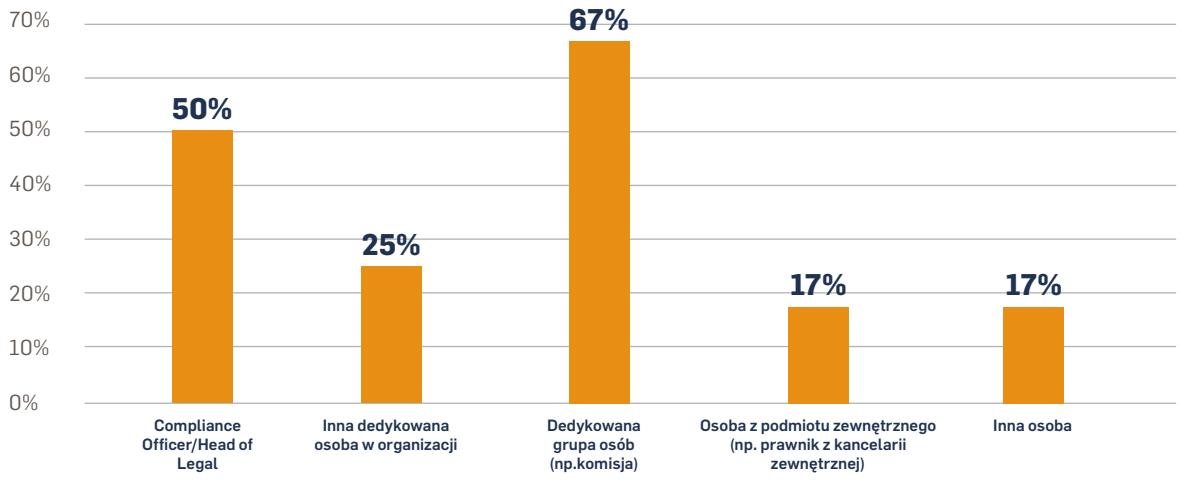
w procedurach do zgłaszania nieprawidłowości, uzupełniane czasami o wypełniane corocznie oświadczenia o braku wiedzy o nieprawidłowościach.

W świetle przepisów karnych projektu ustawy, należy też uświadomić pracowników, że w przypadku:

- utrudniania dokonanie zgłoszenia,
- podejmowania działań odwetowych,
- naruszenia obowiązku zachowania poufności,
- zgłoszenie lub ujawnienia nieprawdziwych informacji;

mogą czekać ich konsekwencje prawnokarne, gdy ich działania będą nosić znamiona umyślności. W przypadku gdy szeregowi pracownicy zostaną odpowiednio przeszkoleni, a organizacja wdroży odpowiednie procedury i będzie prowadzić postepowania wyjaśniające z należytą starannością, odpowiedzialność za naruszenia będzie ciążyła najprawdopodobniej głównie na naruszycielach. Większość organizacji posiadających utrwalone praktyki whistleblowingowe dąży do tego, aby poczucie odpowiedzialności za prawidłowe funkcjonowanie systemu spoczywało na wszystkich pracownikach.

Osoba odpowiedzialna za proces rozpatrywania zgłoszeń



Zobowiązanie do poufności

Ponieważ Dyrektywa jak i polskie ustawy największy nacisk kładzie na zapewnienie poufności i bezpieczeństwa sygnalistom, istotne jest też zadbanie o te kwestie również przy delegowaniu zadań innym osobom w organizacji. Gdy postępowanie wyjaśniające jest skomplikowane, nieuchronnie zaczyna angażować coraz więcej innych osób w organizacji. Istotne jest zatem zadbanie by mimo zwiększania się liczby osób mających wiedzę o nieprawidłowości, dbać o poufność i bezpieczeństwo sygnalisty i wrażliwych informacji. Zgodnie z najlepszą praktyką rynkową, w przypadku pracowników, którzy nie są członkami komisji wyjaśniających lub nie są odpowiednio przeszkoleni, firmy mogą stosować obowiązek podpisywania zobowiązań do poufności, określające również konsekwencje osobiste działania z narażeniem sygnalisty. Należy też zawsze rozważyć, na ile informacja o szczegółach zgłoszenia jest potrzebna danej osobie i na ile dane zadanie może być wykonane bez takiej wiedzy.

Kwestie te są również szeroko poruszane w projekcie ustawy, który w art. 30 ust. 2 wyraźnie stanowi, że do przyjmowania i weryfikacji zgłoszeń, podejmowania działań następczych oraz przetwarzania danych osobowych osób, mogą być dopuszczone wyłącznie osoby posiadające pisemne upoważnienie pracodawcy. Dobrą praktyką rynkową byłoby dołączanie do takiego upoważnienia pisemnych zobowiązań do poufności, co pozwoli wykazywać dodatkową należytą staranność w zakresie dbania o ochronę tożsamości sygnalisty. Takie działanie ma przede wszystkim charakter uświadamiający.

CZEGO POTRZEBUJE BIZNES?

Szczególne kontrowersje w projekcie ustawy budzą surowe sankcje karne za złamanie jej przepisów (nawet do 3 lat pozbawienia wolności). Ryzyko poniesienia odpowiedzialności karnej ciąży głównie:

- na osobie odpowiedzialnej za wdrożenie i funkcjonowanie systemu whistleblowingowego
- na kadrze zarządzającej - w związku z niedopełnieniem obowiązku stworzenia systemu lub jego nieprawidłowe stworzenie i utrudnianie dokonywania zgłoszeń,
- na naruszycielach i innych pracownikach – w związku z dopuszczeniem się np. działań odwetowych czy ujawnienia tożsamości, utrudniania dokonywania zgłoszeń,
- na osobie, która ujawniła nieprawdziwe informacje.

Ponieważ ustawa nie wymaga ustalenia osób odpowiedzialnych za nadzór nad systemem, odpowiedzialność karna za naruszenia nie jest jasno rozłożona w ramach organizacji i co do zasady może spoczywać w pierwszej kolejności na przedstawicielach top managementu oraz dalej na osobach odpowiedzialnych za kwestie prawne i HR-owe. Przydatne w tym zakresie byłby wskazówki, w jaki sposób kadra zarządzająca mogłaby delegować odpowiedzialność osobistą "w dół" organizacji - np. na osoby odpowiedzialne za poszczególne działania w systemie whistleblowingowym w organizacji, a nawet wyłącznie na naruszycielu (gdy np. organizacja jest w stanie wykazać należytą staranność w zakresie przeciwdziałania wystąpieniu działań odwetowych).

Zbytnio dotkliwa wydaje się szczególnie sankcja za zgłoszenie nieprawdziwych informacji. Co prawda przestępstwa zawarte w ustawie wymagają umyślności działania - więc pociągnięcie do odpowiedzialności karnej osoby, która zgłosiła nieprawdziwe w informacje w dobrej wierze, nie powinno być możliwe - to istnienie przepisu karnego sankcjonującego nieprawdziwe zgłoszenia, a szczególnie jego tak ogólne sformułowanie, tworzy istotną barierę sygnalizowania. Może ona wyłącznie zniechęcać do dokonywania zgłoszeń. Szczególnie osoby, które chcą zgłosić podejrzenie nieprawidłowości, na której istnienie nie mają dowodów. Pomocne mogłoby tu być doprecyzowane pojęcia dobrej/złej wiary w działaniu sygnalisty.

6. KATALOG NARUSZEŃ W SYSTEMIE WHISTLEBLOWING

Co powinno trafiać do systemu?

Zgodnie z art. 3 projektu ustawy, do systemu whistleblowing powinny trafiać informacje o **nieprawidłowościach**[1], tam zwane naruszeniem prawa, które jest działaniem lub zaniechaniem niezgodnym z prawem lub mającym na celu obejście prawa, pozostające w związku z pracą i dotyczące w szczególności:

a. zamówień publicznych;
b. usług, produktów i rynków finansowych;
c. zapobiegania praniu pieniędzy i finansowaniu terroryzmu;
d. bezpieczeństwa produktów i ich zgodności z wymogami;
e. bezpieczeństwa transportu;
f. ochrony środowiska;
g. ochrony radiologicznej i bezpieczeństwa jądrowego;
h. bezpieczeństwa żywności i pasz;
i. zdrowia i dobrostanu zwierząt;
j. zdrowia publicznego;
k. ochrony konsumentów;
l. ochrony prywatności i danych osobowych;
m. bezpieczeństwa sieci i systemów teleinformatycznych;
n. interesów finansowych Unii Europejskiej;
o. rynku wewnętrznego Unii Europejskiej, w tym zasad konkurencji i pomocy państwa oraz opodatkowania osób prawnych.

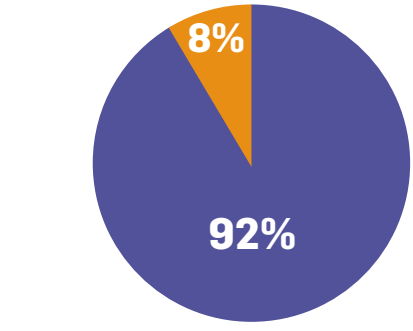
Inne kategorie nieprawidłowości

Pracodawca może dodatkowo ustanowić zgłaszanie w zakładzie pracy innych naruszeń, w tym dotyczących obowiązujących u tego pracodawcy regulacji wewnętrznych lub standardów etycznych. Ponadto wiele firm z sektorów regulowanych dołącza do listy naruszeń podlegających zgłoszeniu także niezgodności z wymogami kodeksów branżowych przyjmowanych w ramach działań samoregulacyjnych.

Jak pokazuje statystyka, zaledwie 8% ankietowanych w badaniu DZP i UNGC wskazuje, że w ramach swoich wewnętrznych systemów whistleblowing dopuszczają możliwość zgłoszenia wyłącznie wybranych rodzajów nieprawidłowości. Regulacja projektu ustawy, wprowadza więc swoisty dualizm sytuacji sygnalistów. Chcąc sprostać wymogom prawnym, pracodawcy mogą ograniczyć katalog nieprawidłowości, które podlegają zgłoszeniu, do minimum wymaganego ustawą. Taki zabieg sprawi, że sytuacja sygnalistów będzie bardzo niepewna. Należy bowiem zaznaczyć, że w katalogu nieprawidłowości z projektu ustawy brakuje m.in. kwestii pracowniczych – np. mobbingu. Zgłaszając takie nieprawidłowości co do zasady nie podlega się ochronie na gruncie projektu ustawy, chyba że pracodawca postanowi inaczej.

Zgłaszanie indywidualnych spraw godzących w interes wyłącznie danego pracownika, jeśli ma nie podlegać zgłoszeniu na zasadach whistleblowingowych, to powinno być uregulowane w odrębnych procedurach wewnętrznych. Zwykle jednak polityki antymobbingowe w organizacjach są przygotowane lakonicznie i rzadko ich przekaz wparty jest dedykowanymi szkoleniami. Wdrożenie procedur whistleblowingowych wyłączających z katalogu dopuszczalnych zgłoszeń indywidualne kwestie pracownicze powinno motywować organizacje do aktualizacji (lub wdrożenia, jeśli takie nie zostały jeszcze przyjęte) regulacji antymobbingowych - spójnych z lub sprawnie funkcjonujących równolegle do systemu whistleblowingowego.

Rodzaje nieprawidłowości, które podlegają zgłoszeniu wewnętrznemu



1 Na potrzeby raportu używamy pojęcia nieprawidłowości, które oznacza zarówno naruszenia prawa krajowego i unijnego, o których mowa w Dyrektywie i projekcie ustawy, jak również inne nieprawidłowości wewnętrzne. Nieprawidłowości stanowią więc również m.in. naruszenie zasad etyki, przyjętych zasad wewnętrznych, wiążących organizację zasad branżowych oraz przyjętych przez środowisko biznesowe standardów działania

CZEGO POTRZEBUJE BIZNES?

Wiele podmiotów wskazuje, że obszary zakreślone w Dyrektywie, z których naruszenie podlega zgłoszeniu, są mało precyzyjne, a paradoksalnie jednocześnie bardzo szerokie w interpretacji. Od polskiego ustawodawcy oczekiwano doprecyzowania przepisów w tym zakresie. Jednym z najszerszych obszarów, które mogą wydawać się dość abstrakcyjne dla sygnalistów to obszar naruszeń w obszarze interesów finansowych UE. Dziwi także fakt niewłączenia w ten katalog przepisów o BHP czy np. bezpieczeństwie produkcji (nie tylko produktów). To jeden z punktów najczęściej dołączanych do listy kategorii naruszeń przez firmy zaangażowane w projekt, szczególnie z sektora produkcyjnego.

7. KOMU I JAK UDOSTĘPNIAĆ SYSTEM?

Kto może dokonać zgłoszenia nieprawidłowości?

Zgodnie z projektem ustawy obowiązek stworzenia wewnętrznych kanałów zgłaszania naruszeń, dotyczy **jedynie umożliwienia dokonywania takich zgłoszeń przez pracowników** w rozumieniu kodeksu pracy oraz pracowników tymczasowych w rozumieniu ustawy o zatrudnianiu pracowników tymczasowych.

W przypadku innych osób niż pracownicy w rozumieniu projektu ustawy, udostępnienie wewnętrznych sposobów zgłaszania naruszeń jest fakultatywne. Wynika to z art. 29 ust. 2 pkt 1 projektu ustawy, który określa, że regulamin zgłoszeń wewnętrznych może (ale nie musi) objąć dodatkowo inne osoby niż pracownicy, od których przyjmowane są zgłoszenia zgodnie z regulaminem zgłoszeń wewnętrznych, takie jak: byli pracownicy, osoby świadczące pracę na rzecz pracodawcy na innej podstawie niż stosunek pracy, akcjonariusze, wspólnicy, członkowie organu zarządzającego lub organu nadzoru, wolontariusze, stażyści oraz osoby pracujące pod nadzorem i kierownictwem wykonawcy, podwykonawcy i dostawcy[1]. Takie rozszerzenie katalogu potencjalnych sygnalistów decyduje się większość firmy, które posiadają już ugruntowane rozwiązania whistleblowingowe.

Co wymaga szczególnego podkreślenia, z uwagi na bardzo szeroką definicję zgłaszającego, która została zawarta w projekcie ustawy i to, że zgłaszający może dokonać zgłoszenia zewnętrznego **bez uprzedniego dokonania zgłoszenia wewnętrznego**, wydaje się zasadne, by w ramach regulaminu zgłoszeń wewnętrznych ustanowionego w organizacji, **jednak umożliwić dokonywanie zgłoszeń nie tylko pracownikom w rozumieniu projektu ustawy, ale każdemu zgłaszającemu.** Może to mieć korzystny wpływ na minimalizację liczby zgłoszeń zewnętrznych lub ujawnień publicznych, które to niejednokrotnie mogą stanowić dla organizacji ryzyko co najmniej PR-owe.

Kwestia anonimowości

Projekt ustawy nie nakłada również obowiązku przyjmowania zgłoszeń anonimowych, a przepisy w tym zakresie stosuje się do zgłoszenia informacji o naruszeniu prawa anonimowo, wyłącznie w przypadkach, gdy możliwość zgłoszenia informacji o naruszeniu prawa anonimowo przewiduje regulamin zgłoszeń wewnętrznych, stosowany przez pracodawcę, określający wewnętrzną procedurę zgłaszania naruszeń prawa lub procedura zgłaszania naruszeń prawa organowi publicznemu. Jeżeli chodzi o inne przepisy prawne w tym zakresie, niż te zawarte w projekcie ustawy, to przedstawione kwestie są ujęte w innych obowiązujących już polskich ustawach stosunkowo wąsko. Przykładowo - ustawa o ofercie publicznej mówi o konieczności udostępniania kanałów anonimowego zgłaszania wyłącznie pracownikom, natomiast ustawa o AML mówi o kanałach anonimowego zgłaszania udostępnianych pracownikom lub innym osobom wykonujących czynności na rzecz instytucji obowiązanej. Co warte podkreślenia, **wszystkie organizacje biorące udział w badaniu DZP i UNGC zadeklarowały, że udostępniają anonimowe kanały zgłaszania.**

W zakresie zgłoszeń zewnętrznych, zgodnie z art. 29 ust. 2 pkt. 5 projektu ustawy, w ramach regulaminu, pracodawca powinien dodatkowo wskazać, że zgłoszenie może w każdym przypadku nastąpić również do organu publicznego lub organu centralnego z pominięciem procedury przewidzianej w regulaminie zgłoszeń wewnętrznych, w szczególności, gdy:

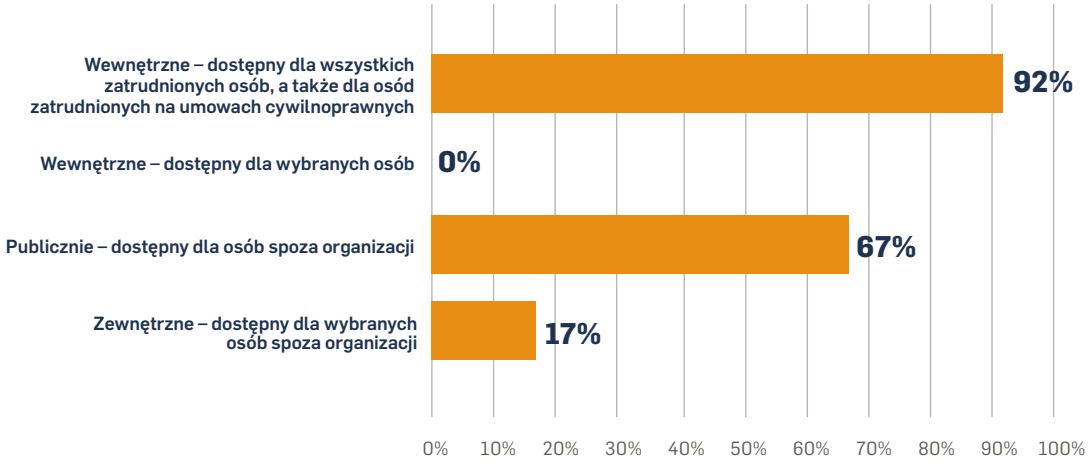
a. w terminie na przekazanie informacji zwrotnej ustalonym w regulaminie zgłoszeń wewnętrznych pracodawca nie podejmie działań następczych lub nie przekaże zgłaszającemu informacji zwrotnej; lub
b. zgłaszający ma uzasadnione podstawy by sądzić, że naruszenie prawa może stanowić bezpośrednie lub oczywiste zagrożenie dla interesu publicznego, w szczególności istnieje ryzyko nieodwracalnej szkody, lub
c. dokonanie zgłoszenia wewnętrznego narazi zgłaszającego na działania odwetowe lub
d. w przypadku dokonania zgłoszenia wewnętrznego istnieje niewielkie prawdopodobieństwo skutecznego przeciwdziałania naruszeniu prawa przez pracodawcę z uwagi na szczególne okoliczności sprawy, takie jak możliwość ukrycia lub zniszczenia dowodów lub możliwość istnienia zmowy między pracodawcą a sprawcą naruszenia prawa lub udziału pracodawcy w naruszeniu prawa.

Zgłoszenie dokonane do organu publicznego lub organu centralnego z pominięciem procedury określonej w ww. regulaminie zgłoszeń wewnętrznych nie skutkuje pozbawieniem zgłaszającego ochrony przewidzianej w projekcie ustawy.

1 Art. 29 ust. 2 pkt 1 pomija wymienione w art. 4 "osoby ubiegające się o zatrudnienie, które uzyskały informację o naruszeniu prawa w procesie rekrutacji lub negocjacji poprzedzających zawarcie umowy.

Projekt ustawy nie przewiduje obowiązku utworzenia kanału dla podmiotów innych niż pracownicy w rozumieniu projektu ustawy, ale zgodnie z przeprowadzonymi ankietami, aż 67% spośród ankietowanych zadeklarowało, że ich organizacja posiada kanały zgłaszania kierowane publicznie, a 17% badanych odpowiedziało, że wdrożone przez nich kanały wewnętrzne są dostępne również dla podmiotów takich jak np. dostawcy, akcjonariusze. Oznacza to, że tylko 16% ankietowanych stosuje wyłącznie wewnętrzne rozwiązania, co pokazuje wysoką świadomość rynku w zakresie korzyści, jakie może dawać posiadanie szeroko udostępnionych kanałów zgłoszeń.

Jak udostępniane są wewnętrzne kanały

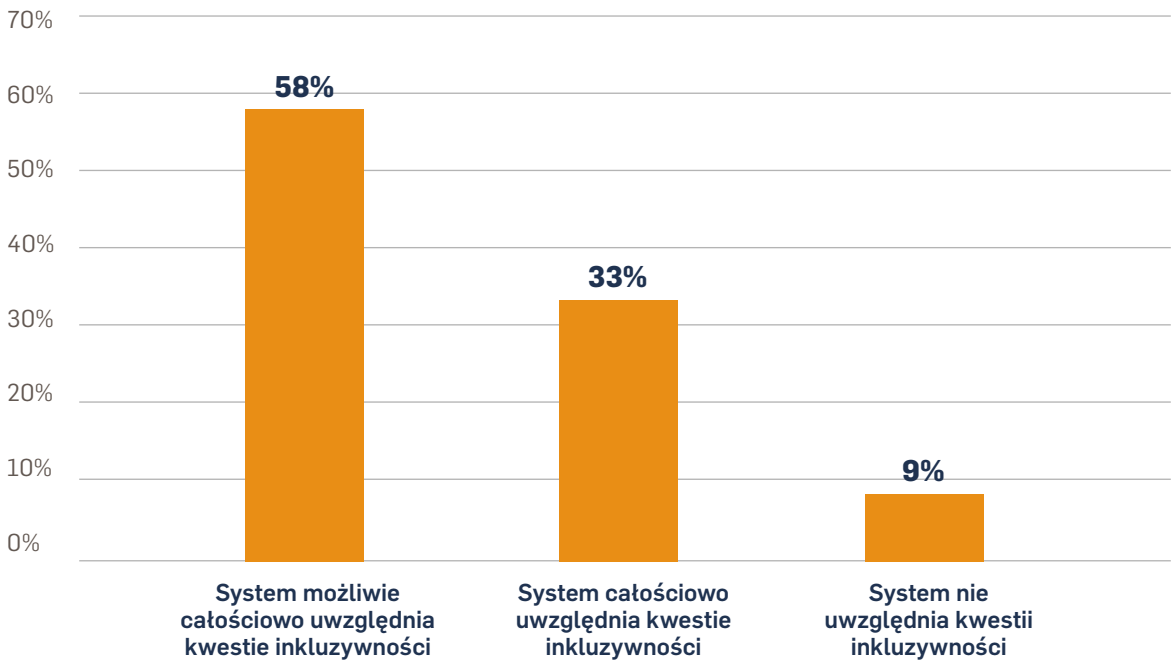


Rozmowy z organizacjami, które nie udostępniają kanałów publicznych, pokazują, że najczęstszym powodem unikania takiego kanału jest obawa przed napływem wielu nierzetelnych zgłoszeń, które konsumują środki działów obsługujących kanały. Co ciekawe, doświadczenia organizacji, które wdrożyły kanały zewnętrzne, pokazują w większości, że obawy te nie są uzasadnione. Liczba zgłoszeń otrzymywanych za pośrednictwem kanałów zewnętrznych nie przekracza liczby zgłoszeń z kanałów wewnętrznych, a stosunek liczby zgłoszeń zewnętrznych zweryfikowanych pozytywnie do tych zweryfikowanych negatywnie przeważnie utrzymuje się na podobnym poziomie jak ten dla zgłoszeń wewnętrznych. Udostępniając kanał wybranym podmiotom (w szczególności kontrahentom, dostawcom) organizacje mogą też iść na kompromis dopuszczając jedynie zgłoszenia od wybranych podmiotów, np. konkretnych firm, którym podano takie dane na poziomie klauzul kontraktowych czy w dedykowanym mailingu informacyjnym. Jest to dobre posunięcie ze strony organizacji, bowiem w praktyce jednak zawsze można spotkać się z sytuacją, gdy do siedziby spółki wpływają listy będące tzw. anonimami, a które i tak muszą zostać wyjaśnione. Gdyby te same osoby zastosowały sformalizowane rozwiązania whistleblowing (jak np. platforma IT) możliwe byłoby np. utrzymywanie z nimi kontaktu i łatwiejsze wykazywanie należytej staranności w wyjaśnianiu sprawy, a także zapewnienie, że informacja trafi do konkretnej, wyznaczonej w organizacji osoby, uprawnionej do odbierania takich zgłoszeń.

Kwestia inkluzywności

Zastanawiając się nad kształtem poszczególnych kanałów zgłaszania, warto pochylić się również na chwilę nad poziomem ich inkluzywności. W szczególności ze względu na wiek, niepełnosprawności czy wykluczenie cyfrowe potencjalnych użytkowników systemu whistleblowing. Jak pokazuje badanie, coraz więcej organizacji samodzielnie decyduje się na takie skonstruowanie systemu, by chociaż częściowo zaadresować te kwestie – niemal 60% spośród badanych zadeklarowało, że tworząc swój system zgłaszania nieprawidłowości kierowało się względami inkluzywności. Tworzy się specjalne skrzynki dla pracowników pracujących na halach produkcyjnych, niemających dostępu do sprzętu służbowego, czy korzysta się nawet z rozwiązań internetowych, ułatwiających nawigację po stronie osobom niewidomym z wykorzystaniem translatorów tekstu na mowę.

Inkluzywny sposób budowania systemów zgłaszania nieprawidłowości, który uwzględnia takie problemy jak np. wykluczenie cyfrowe, wiek, niepełnosprawność



CZEGO POTRZEBUJE BIZNES?

Kwestią mogącą wymagać uregulowania jest relacja publicznego kanału udostępnianego przez prywatną organizację (niewymaganego projektem ustawy) do wewnętrznego (który musi spełniać wymagania projektu). By nie zniechęcać podmiotów prywatnych do tworzenia takich kanałów, ustawodawca powinien wyraźnie rozdzielić te dwie sytuacje i określić ich wzajemną relację.

Inna ciekawa kwestia dotyczy liczenia stanu zatrudnienia w organizacji, co najczęściej dotyczy firm korzystających z pracowników tymczasowych, których liczba jest zmienna w ciągu roku. Jeżeli organizacje są na skraju progów zatrudnienia (50 lub 250 osób), czy zmniejszając zatrudnienie i wychodząc spod zastosowania ustawy, można przyjmować, że nie ma obowiązku stosować wymogów ustawy? Kluczowe pytanie to, na jaki moment liczyć stan zatrudnienia i jak często należy to weryfikować.

Analogiczna sytuacja dotyczy pytania o standard ochrony zgłaszających innych niż pracownicy, którym fakultatywnie udostępnia się wewnętrzny kanał zgłoszeń. Czy ustawa wymaga wtedy by pracodawca chronił taką osobę przed pełnym katalogiem działań odwetowych – w tym np. przed zwolnieniem? W jaki praktyczny sposób pracodawca ma realizować taki obowiązek w stosunku do osób pracujących pod nadzorem i kierownictwem wykonawcy, podwykonawcy i dostawcy? Kwestie te powinny być szczegółowiej uregulowane – najlepiej z korzyścią dla pracodawcy, który chce wyjść naprzeciw innym podmiotom, w stosunku do których nie jest zobowiązany do udostępniania kanałów zgłaszania. W innym wypadku, niepewność co do stosowania prawa w tym zakresie, może spowodować ograniczanie powszechnego udostępniania kanałów zgłoszeń szerszej liczbie podmiotów.

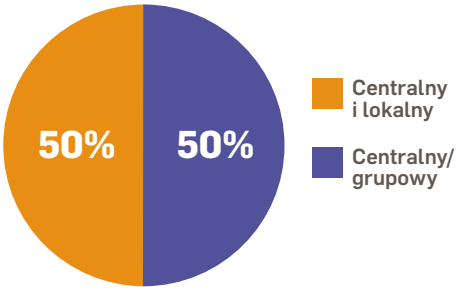
8. ORGANIZACJA SYSTEMU WHISTLEBLOWING W PODMIOTACH POWIĄZANYCH

Kwestią, która wzbudza wiele kontrowersji w związku z implementacją Dyrektywy o ochronie sygnalistów, jest ukształtowanie systemów zgłaszania nieprawidłowości w grupach kapitałowych i podmiotach powiązanych. Do tej pory popularnym modelem było wdrożenie kanałów whistleblowingowych na poziomie centralnym – pracownicy wszystkich „spółek córek" mogli sygnalizować nieprawidłowości wyznaczonej komórce organizacyjnej lub osobie w „spółce matce". Często korzystano jednocześnie z outsourcingu w zakresie przyjmowania zgłoszeń – przeważnie jednak „centrala" odpowiedzialna była za dalsze procedowanie zgłoszenia.

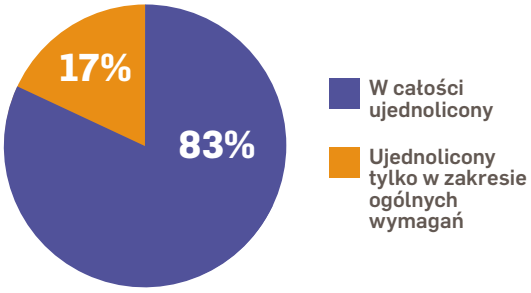
100% ankietowanych podmiotów przynależących do grup kapitałowych zadeklarowało, że umożliwia dokonywanie zgłoszeń za pomocą kanału centralnego – 50% że wdrożyło także kanały lokalne.

83% podmiotów wskazało przy tym, że proces zgłaszania nieprawidłowości jest w obrębie grupy całkowicie ujednolicony – 17%, że jest ujednolicony tylko w zakresie ogólnych wymagań.

Kanały zgłaszania nieprawidłowości



Ujednolicenie kształtu procesu zgłaszania nieprawidłowości w ramach grupy kapitałowej



Jakie jest stanowisko Komisji Europejskiej?

Wątpliwości co do zgodności tego rozwiązania z Dyrektywą powstały na gruncie art. 8 ust. 3, który nakłada obowiązek ustanowienia kanałów i procedur na potrzeby zgłaszania nieprawidłowości na podmioty prawne w sektorze prywatnym zatrudniające 50 i więcej pracowników. Komisja Europejska zaadresowała tę kwestię w listach do przedsiębiorców z dni 2 i 26 czerwca 2021 r.

Organ stanął na stanowisku, że przepis ten powinien być interpretowany ściśle – podmioty należące do grup kapitałowych również są objęte zakresem jego zastosowania. Każda ze spółek musi posiadać własne kanały zgłaszania nieprawidłowości. Komisja zaznacza przy tym, że optymalnym jest, żeby sygnalista mógł zgłosić nieprawidłowość nie tylko na poziomie spółki, ale również bezpośrednio grupie – kanały lokalne i centralne mogą zatem funkcjonować równolegle.

Postępowanie wyjaśniające w sprawie zgłoszenia dokonanego lokalnie powinno być prowadzone na poziomie tej samej spółki. Gdyby okazało się, że ujawnia ono problem strukturalny, który dotyczy kilku podmiotów w obrębie grupy i uzasadnione jest jego kooperatywne rozpatrzenie, spółka która zgłoszenie otrzymała powinna wystąpić o zgodę sygnalisty na przekazanie informacji nim objętych dalszym interesariuszom. Sygnalistę należałoby również informować o możliwości wycofania zgłoszenia w braku takiej zgody.

Komisja uważa także, że dzielenie się zasobami na potrzeby wyjaśnienia zgłoszeń przez „spółkę-matkę" ze „spółkami-córkami" w świetle Dyrektywy dopuszczalne jest tylko co do podmiotów średniej wielkości (od 50 do 249 pracowników) i przy spełnieniu następujących przesłanek:

• na poziomie „spółki-córki" istnieją kanały zgłaszania nieprawidłowości,
• sygnalista jest informowany, że jego zgłoszenie zostanie rozpoznane przez „spółkę-matkę" oraz może się temu sprzeciwić i zażądać wyjaśnienia na poziomie lokalnym,
• działania następcze podejmowane są na poziomie lokalnym i z tego też poziomu sygnalista otrzymuje feedback.

Projekt ustawy przewiduje możliwość dzielenia się zasobami przez podmioty średniej wielkości, nie adresując kwestii powiązań między nimi. Współdziałanie takie miałoby się odbywać na podstawie umowy i przy spełnieniu przesłanki przekazywania informacji zwrotnej i podejmowania działań następczych na poziomie lokalnym. Projekt nie rozwiewa natomiast wątpliwości co do dopuszczalności stosowania wyłącznie scentralizowanych kanałów zgłaszania nieprawidłowości. Bezpiecznie jest zatem przyjąć, że przepisy ustawy powinny być interpretowane w duchu stanowiska KE.

Na czym polega outsourcing usług związanych z whistleblowingiem?

Komisja potwierdziła, że usługi związane ze zgłaszaniem nieprawidłowości można outsourcować. Podmiot zewnętrzny może w tym wypadku przyjmować zgłoszenia i dokonywać ich wstępnej weryfikacji. Odpowiedzialność za rozpatrywanie zgłoszeń i wdrożenie działań naprawczych w dalszym ciągu spoczywa jednak na organizacji (co nie oznacza, że nie może ona w tym procesie korzystać ze wsparcia profesjonalnych doradców).

Projekt ustawy także przewiduje możliwość powierzenia czynności związanych z przyjmowaniem zgłoszeń oraz podejmowaniem działań następczych podmiotowi zewnętrznemu pod warunkiem zawarcia umowy. Podmiot zewnętrzny musi także zapewniać wykonanie tych czynności z zastosowaniem rozwiązań technicznych i organizacyjnych zapewniających ich zgodność z ustawą. Jednocześnie nie zwalnia to jednak pracodawcy z odpowiedzialności za system.

Odbiór stanowiska

Dania, państwo, które na dzień sporządzenia raportu zaimplementowało Dyrektywę, zdecydowało, aby zezwolić grupom kapitałowym na korzystanie wyłącznie z kanałów scentralizowanych. Wpływ na to miały informacje zwrotne od interesariuszy – przedsiębiorców. Ustawodawca zaznaczył jednak, że jeśli inne kraje przyjmą rozwiązanie przeciwne, a Komisja podtrzyma swój pogląd, gotów jest znowelizować przyjęte przepisy.

Nasze spostrzeżenia

Dyrektywa w żaden sposób nie odnosi się do modelu biznesowego, jakim jest franczyza. W związku ze specyfiką tego rozwiązania, w interesie organizatora sieci zdaje się przyjmowanie zgłoszeń od pracowników franczyzobiorców. W świetle Dyrektywy oraz projektu ustawy zdaje się to dopuszczalne, pod warunkiem odpowiedniego ukształtowania systemu whistleblowing przez franczyzodawcę.

CZEGO POTRZEBUJE BIZNES?

Jak zostało wspomniane wyżej - Dania zdecydowała się na umożliwienie korzystania wyłącznie z kanałów scentralizowanych – jak wynika z naszego badania również w Polsce istnieją firmy, które zdecydowały się na takie rozwiązanie. Istotnym byłoby wysłuchanie przez ustawodawcę głosu biznesu i motywów stojących za decyzją o stosowaniu wyłącznie scentralizowanych kanałów zgłaszania nieprawidłowości i wyważenie interesów sygnalistów oraz pracodawców w końcowym brzmieniu regulacji.

9. INFORMACJA ZWROTNA I KONTAKT Z SYGNALISTĄ

Informacja zwrotna dla sygnalisty – jakie zmiany przyniesie implementacja Dyrektywy?

Przepisy obowiązujące aktualnie w Polsce, nakładające na wybrane podmioty obowiązek posiadania systemów zgłaszania nieprawidłowości, nie przewidują konieczności przekazania sygnaliście informacji zwrotnej. Sytuację tą zmienia procedowany właśnie projekt ustawy. Udzielenie feedbacku zgłaszającemu naruszenie wewnętrznie będzie wymagane na dwóch etapach:

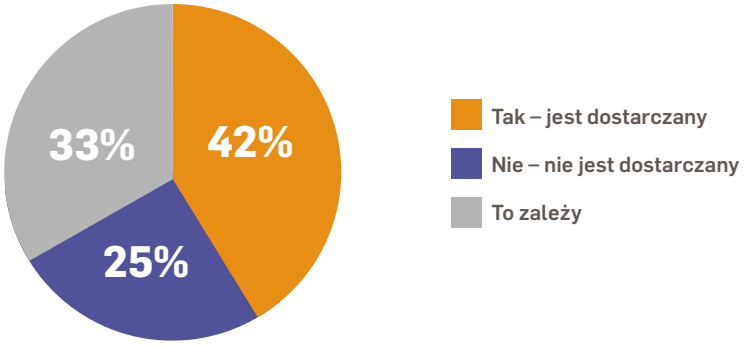
- W terminie 7 dni od dokonania zgłoszenia - potwierdzenie przyjęcia zgłoszenia;
- W terminie nieprzekraczającym trzech miesięcy od dokonania zgłoszenia (lub, w braku uprzedniego potwierdzenia jego przyjęcia – trzech miesięcy od upływu 7 dni od dokonania zgłoszenia) - informacja o podjętych działaniach następczych w związku ze zgłoszeniem.

Zdaje się przy tym, że mówiąc o potwierdzeniu przyjęcia zgłoszenia, nie chodzi o automatyczne potwierdzenie generowane przez system, ale rzeczywiste działanie osoby odpowiedzialnej za przyjmowanie zgłoszeń, najlepiej po co najmniej wstępnej weryfikacji zgłoszenia.

Dobre praktyki rynkowe

Aż 75% firm, które wzięły udział w badaniu zadeklarowało, że przekazuje sygnaliście informację zwrotną, choć 33% z nich uzależnia to od dodatkowych przesłanek, najważniejszą z których jest podanie przez sygnalistę swoich danych.

Organizacja przekazuje sygnaliście feedback



Wszyscy ankietowani wskazywali, że udzielają informacji zwrotnej po zakończeniu postępowania wszczętego w celu podjęcia działań następczych po dokonaniu zgłoszenia. Większość podmiotów deklarowała również, że przekazuje sygnaliście feedback po otrzymaniu zgłoszenia, a niektóre - że w toku postępowania informują, na jakim jest ono etapie.

Jakie informacje przekazywać?

Zgodnie z projektem ustawy, informacja zwrotna, udzielana sygnaliście w terminie nieprzekraczającym trzech miesięcy od dokonania zgłoszenia, obejmuje w szczególności informację o:

- stwierdzeniu bądź braku stwierdzenia wystąpienia naruszenia prawa i
- ewentualnych środkach, które zostały lub zostaną zastosowane w reakcji na stwierdzone naruszenie prawa.

Dyrektywa w motywie 57 doprecyzowuje jakie jeszcze informacje powinny być przekazywane w ramach ta-

kich działań. Działania następcze mogą obejmować, na przykład, skierowanie sprawy do innych kanałów lub procedur, zakończenie procedury z powodu braku wystarczających dowodów lub z innych powodów, wszczęcie dochodzenia wewnętrznego czy dokonane w jego toku ustalenia lub środki podjęte w celu zaradzenia podniesionej kwestii, przekazanie sprawy do właściwego organu w celu przeprowadzenia dalszego postępowania wyjaśniającego.

W dyrektywie zastrzega się jednak, że informacje te powinny pozostawać bez uszczerbku dla dochodzenia wewnętrznego lub postępowania wyjaśniającego lub dla praw osoby, której dotyczy zgłoszenie. W ramach dobrych praktyk, warto pamiętać, że nie ma obowiązku przekazywania sygnaliście informacji sensytywnych czy dokładnej relacji z przebiegu postępowania wyjaśniającego. Oznacza to, że udzielając feedbacku końcowego należy mieć na względzie też dobro i interes organizacji.

Korzyści z przekazywania informacji zwrotnej

Przekazywanie sygnaliście feedbacku to nie tylko wymóg projektu ustawy, ale też praktyka, która pociąga za sobą szereg korzyści:

- buduje zaufanie zgłaszających do systemu whistleblowingewego – otrzymując informację zwrotną sygnalista ma pewność, że zgłoszenie zostało potraktowane poważnie, a w związku z jego wpływem podjęto odpowiednie kroki;
- pomaga kształtować kulturę speak-up;
- mobilizuje do podejmowania odpowiednich działań w związku z otrzymaniem zgłoszenia.

Pozostawanie w kontakcie ze zgłaszającym może okazać się bardzo korzystne dla organizacji. Sygnalista może mieć wiedzę o dalszych poczynaniach osoby dopuszczającej się nadużyć. Osoby odpowiedzialne za weryfikację i rozpatrzenie zgłoszenia mogą również mieć potrzebę uściślenia lub wyjaśnienia pewnych wskazanych przez sygnalistę faktów.

Dlatego dobrą praktyką jest zaznaczenie potrzeby pozostania w kontakcie na poziomie procedury lub w formularzu zgłoszeniowym.

CZEGO POTRZEBUJE BIZNES?

W przypadku gdy organizacja umożliwia zgłaszanie anonimowe (a może choć nie musi tego zrobić) – zgodnie z obecnym projektem ustawy – może nie być jasne, czy na organizacji dalej ciąży obowiązek udzielenia informacji zwrotnej dla zgłoszeń anonimowych. W praktyce, jeżeli sygnalista nie poda w zgłoszeniu danych kontaktowych, tylko niektóre kanały zgłaszania umożliwią utrzymanie kontaktu z sygnalistą i udzielanie informacji zwrotnych. Obecnie wydaje się, że przepisy należy interpretować z korzyścią dla organizacji udostępniającej kanały anonimowe. To znaczy, że przy udostepnieniu możliwości zgłaszania anonimowego, nie mamy automatycznego obowiązku udzielania feedbacku, szczególnie jeżeli nie jest to fizycznie możliwe (o ile organizacja udostępnia również inne kanały poufne zgodne z ustawą). Przepisy mówią, że anonimowy sygnalista, którego tożsamość zostanie ujawniona w dalszych etapach procedowania zgłoszenia uzyskuje prawa ochronne takie jak sygnalista, który podałby swoje dane. Poprzez analogię prawo dostępu do informacji zwrotnej mogłoby działać na takiej samej zasadzie. To znaczy, że organizacja udzielałaby wcześniej anonimowym sygnalistom feedback dopiero przy ewentualnym ujawnieniu ich danych na późniejszych etapach. Wysokie ryzyko generuje bowiem fakt przekazania informacji zwrotnej na podany przez anonimowego sygnalistę adres kontaktowy (np. e-mail spoza domeny organizacji), a organizacja nie ma możliwości upewnienia się, że zgłoszenia na pewno dokonuje pracownik, a nie np. osoba z zewnątrz, której przekazanie szczegółowych informacji zwrotnych może nie leżeć w interesie organizacji i generować potencjalne ryzyko. Kwestia ta powinna zostać dokładniej uregulowana. Szczególnie, że inne polskie ustawy (np. ustawa o AML) nakłada obowiązek wdrożenie kanałów anonimowych i organizacje mogą mieć problem z połączeniem wymogów nakładanych przez różne ustawy.

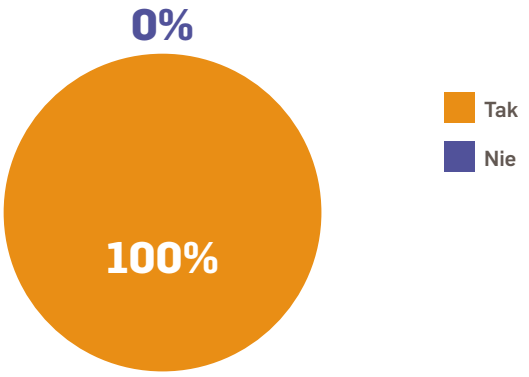
10. ANONIMOWOŚĆ SYGNALISTY A POUFNOŚĆ ZGŁOSZENIA

Z treści art. 16 Dyrektywy i art. 30 projektu ustawy wynika obowiązek zachowania poufności sygnalisty. Oznacza to zapewnienie, że tożsamość osoby dokonującej zgłoszenia nie zostanie ujawniona bez wyraźnej zgody tej osoby – innym osobom, niż osobom wyznaczonym do rozpatrywania zgłoszeń i podejmowania działań następczych. Ustawodawca unijny podkreśla, że zasada ta ma zastosowanie nie tylko do imienia i nazwiska sygnalisty, ale także do innych informacji, na podstawie których można bezpośrednio lub pośrednio zidentyfikować jego tożsamość.

Informacje te mogą zostać ujawnione jedynie wtedy, gdy takie ujawnienie jest koniecznym i proporcjonalnym obowiązkiem prawnym w kontekście prowadzonych przez organy krajowe postępowań wyjaśniających lub postępowań sądowych, w tym w celu zagwarantowania prawa do obrony przysługującego osobie, której dotyczy zgłoszenie. Zanim jednak tożsamość sygnalisty zostanie ujawniona, należy go o tym fakcie powiadomić, wyjaśniając pisemnie powód ujawnienia poufnych danych - wyjątkiem jest jedynie sytuacja, gdy takie powiadomienie mogłoby zagrozić powiązanemu postępowaniu wyjaśniającemu lub postępowaniu sądowemu.

Podmioty zobowiązane na podstawie Dyrektywy oraz projektu ustawy mają umożliwić poufne zgłaszanie nieprawidłowości, ale nic nie stoi na przeszkodzie, aby ustawodawca czy nawet pracodawca zagwarantował sygnalistom możliwość anonimowego informowania o nieprawidłowościach – czyli możliwość dokonania zgłoszenia bez podania własnych danych osobowych. Wszyscy ankietowani w badaniu DZP i UNGC wskazali, że w ramach wdrożonych w swoich organizacjach systemów whistleblowing umożliwiają dokonywanie zgłoszeń anonimowych. Poufność w tym przypadku oznaczać będzie dokonanie zgłoszenia z podaniem swoich danych przez sygnalistę, które to dane nie będą podlegały ujawnieniu podmiotom innym niż zaangażowane w obsługę zgłoszenia.

Możliwość anonimowego dokonywania zgłoszeń wewnętrznych



Niezależnie od tego, czy sygnalista zdecyduje się podać swoje dane w zgłoszeniu czy nie – postępowania wyjaśniające prowadzi się z uwzględnieniem konieczności zapewnienia ochrony tożsamości sygnalisty. Zarówno zgłoszenie anonimowe jak i zgłoszenie z podaniem danych przez sygnalistę wiąże się jednak z określonymi konsekwencjami dla osób rozpatrujących zgłoszenie i prowadzących wewnętrzne postępowanie wyjaśniające. W przypadku zgłoszeń anonimowych sygnalista ma komfort psychiczny, nie obawia się działań odwetowych i w konsekwencji jest bardziej skłonny do dokonania zgłoszenia. Z drugiej jednak strony, w przypadku zgłoszeń anonimowych komunikacja z sygnalistą może być utrudniona, a także wiarygodność zgłoszenia jest mniejsza.

CZEGO POTRZEBUJE BIZNES?

W przypadku gdy organizacja umożliwia zgłaszanie anonimowe (a może choć nie musi tego zrobić) – zgodnie z obecnym projektem ustawy – może nie być jasne, czy na organizacji dalej ciąży obowiązek udzielenia informacji zwrotnej dla zgłoszeń anonimowych. W praktyce, jeżeli sygnalista nie poda w zgłoszeniu danych kontaktowych, tylko niektóre kanały zgłaszania umożliwią utrzymanie kontaktu z sygnalistą i udzielanie informacji zwrotnych. Obecnie wydaje się, że przepisy należy interpretować z korzyścią dla organizacji udostępniającej kanały anonimowe. To znaczy, że przy udostepnieniu możliwości zgłaszania anonimowego, nie mamy automatycznego obowiązku udzielania feedbacku, szczególnie jeżeli nie jest to fizycznie możliwe (o ile organizacja udostępnia również inne kanały poufne zgodne z ustawą). Przepisy mówią, że anonimowy sygnalista, którego tożsamość zostanie ujawniona w dalszych etapach procedowania zgłoszenia uzyskuje prawa ochronne takie jak sygnalista, który podałby swoje dane. Poprzez analogię prawo dostępu do informacji zwrotnej mogłoby działać na takiej samej zasadzie. To znaczy, że organizacja udzielałaby wcześniej anonimowym sygnalistom feedback dopiero przy ewentualnym ujawnieniu ich danych na późniejszych etapach. Wysokie ryzyko generuje bowiem fakt przekazania informacji zwrotnej na podany przez anonimowego sygnalistę adres kontaktowy (np. e-mail spoza domeny organizacji), a organizacja nie ma możliwości upewnienia się, że zgłoszenia na pewno dokonuje pracownik, a nie np. osoba z zewnątrz, której przekazanie szczegółowych informacji zwrotnych może nie leżeć w interesie organizacji i generować potencjalne ryzyko. Kwestia ta powinna zostać dokładniej uregulowana. Szczególnie, że inne polskie ustawy (np. ustawa o AML) nakłada obowiązek wdrożenie kanałów anonimowych i organizacje mogą mieć problem z połączeniem wymogów nakładanych przez różne ustawy.

11. OCHRONA SYGNALISTÓW

Kto podlega ochronie jako sygnalista?

Jak wskazaliśmy w rozdziale 7, przewidzianą przez przepisy Dyrektywy oraz projektu ustawy ochroną objęte są osoby dokonujące:

- zgłoszenia wewnętrznego,
- zgłoszenia zewnętrznego,
- ujawnienia publicznego,

które **uzyskały informacje dotyczące naruszeń w kontekście związanym z pracą w sektorze publicznym lub prywatnym i mogą doświadczyć działań odwetowych w związku ze zgłoszeniem.**

Projekt ustawy, choć posługuje się innymi definicjami, zakreśla taki sam zakres podmiotowy.

Pracownicy w rozumieniu TFUE	Wszelkie osoby wykonujące pracę na rzecz pracodawcy pod jego kierownictwem i za wynagrodzeniem, niezależnie od podstawy prawnej tego stosunku (może to być zarówno umowa o pracę, jak i umowy cywilnoprawne - zlecenie, o świadczenie usług etc.)
Osoby prowadzące działalność gospodarczą na własny rachunek w rozumieniu TFUE (osoby samozatrudnione)	
Akcjonariusze lub wspólnicy spółek, a także członkowie organów zarządzających, nadzorczych iadministracyjnych przedsiębiorstw	
Osoby pracujące pod nadzorem i kierownictwem dostawców, wykonawców i podwykonawców	
Wolontariusze, praktykanci i stażyści – uzyskiwanie wynagrodzenia za wykonywaną pracę nie stanowi przesłanki ochrony	

WAŻNE!
Sygnalista jest objęty ochroną w świetle Dyrektywy, jak również projektu ustawy, jeśli w momencie dokonywania zgłoszenia miał uzasadnione podstawy sądzić, że informacje, które przekazuje są prawdziwe.

Co oznacza „kontekst związany z pracą”?

Sformułowanie to oznacza, że informacja o naruszeniach podjęta została w związku z wykonywaniem pracy – obecnie, w przyszłości lub przeszłości. Ochronie podlegają zatem również byli pracownicy oraz kandydaci w toku rekrutacji.

Chroniona także pomoc w dokonaniu zgłoszenia

Dyrektywa oraz projekt ustawy przewidują ponadto, że ochronie podlegają także osoby, które pomagają sygnaliście w dokonaniu zgłoszenia oraz wszelkim innym osobom trzecim, powiązanym z osobami dokonującymi zgłoszenia, które z uwagi na działania sygnalisty mogą doświadczyć działań odwetowych w kontekście związanym z ich pracą, jak np. współpracownicy lub członkowie rodzin osób dokonujących zgłoszenia.

Działania odwetowe

Zapewnienie bezpieczeństwa zgłaszającym należy do podstawowych przesłanek efektywności systemu whistleblowingowego. Obawa przed działaniami odwetowymi stanowi jedną z najczęstszych przyczyn wstrzymujących sygnalistów przed zgłoszeniem nieprawidłowości.

Działania odwetowe zostały w Dyrektywie zdefiniowane jako bezpośrednie lub pośrednie działania lub zaniechania mające miejsce w kontekście związanym z pracą, spowodowane zgłoszeniem wewnętrznym, zewnętrznym lub ujawnieniem publicznym wyrządzające lub mogące wyrządzić nieuzasadnioną szkodę dla osoby dokonującej zgłoszenia.

Projekt ustawy przewiduje otwarty katalog działań odwetowych w kontekście osób świadczących pracę na podstawie umowy o pracę. Działaniem odwetowym jest nie tylko podjęcie, ale także groźba lub próba podjęcia którejś z poniższych czynności względem sygnalisty:

- odmowa nawiązania stosunku pracy
- wypowiedzenie lub rozwiązanie bez wypowiedzenia stosunku pracy
- niezawarcie umowy o pracę na czas określony po rozwiązaniu umowy o pracę na okres próbny, niezawarcie kolejnej umowy o pracę na czas określony lub niezawarcie umowy o pracę na czas nieokreślony, po rozwiązaniu umowy o pracę na czas określony – w sytuacji gdy pracownik miał uzasadnione oczekiwanie, że zostanie z nim zawarta taka umowa
- obniżenie wynagrodzenia za pracę
- wstrzymanie awansu albo pominięcie przy awansowaniu
- pominięcie przy przyznawaniu innych niż wynagrodzenie świadczeń związanych z pracą
- przeniesienie pracownika na niższe stanowisko pracy
- zawieszenie w wykonywaniu obowiązków pracowniczych lub służbowych
- przekazanie innemu pracownikowi dotychczasowych obowiązków pracowniczych
- niekorzystną zmianę miejsca wykonywania pracy lub rozkładu czasu pracy
- negatywną ocenę wyników pracy lub negatywną opinię o pracy
- nałożenie lub zastosowanie środka dyscyplinarnego, w tym kary finansowej, lub środka o podobnym charakterze
- wstrzymanie udziału lub pominięcie przy typowaniu do udziału w szkoleniach podnoszących kwalifikacje zawodowe
- nieuzasadnione skierowanie na badanie lekarskie, w tym badania psychiatryczne, o ile przepisy odrębne przewidują możliwość skierowania pracownika na takie badanie
- działanie zmierzające do utrudnienia znalezienia w przyszłości zatrudnienia w danym sektorze lub branży na podstawie nieformalnego lub formalnego porozumienia sektorowego lub branżowego

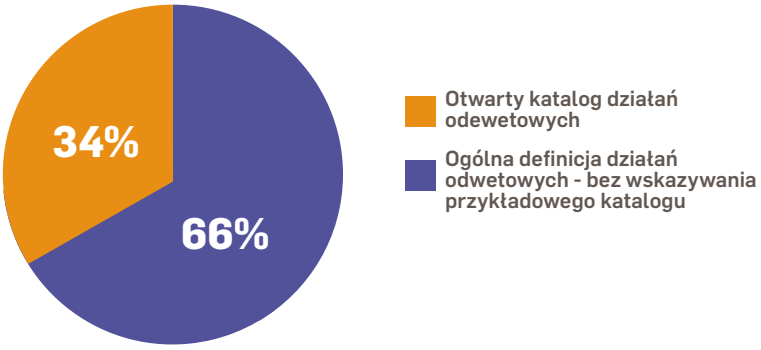
W przypadku, gdy pracodawca zastosuje któryś ze wskazanych wyżej środków względem sygnalisty w oparciu o obiektywne przesłanki obowiązany jest także do udowodnienia tego faktu.

Jeżeli sygnalista nie jest związany stosunkiem pracy, ale innym stosunkiem prawnym, wówczas projekt ustawy wskazuje, że zgłaszający nie może być niekorzystnie traktowany z powodu dokonania zgłoszenia lub ujawnienia publicznego i jako przykłady takich zachowań wskazane są rozwiązanie, wypowiedzenie lub odmowę nawiązania stosunku prawnego, na podstawie którego jest lub ma być świadczona praca przez zgłaszającego.

Projekt ustawy zapewnia także sygnaliście wolność od odpowiedzialności prawnej za szkody wyrządzone dokonaniem zgłoszenia oraz za naruszenie informacji niejawnych, które to zagadnienie poruszone zostało w rozdziale 3 raportu.

Żadna z firm biorących udział w badaniu nie zdecydowała się na wskazanie konkretnego zamkniętego katalogu zachowań, które byłyby definiowane jako działania odwetowe. Dominujące są dwa rozwiązania w tym zakresie. Wskazanie przykładowego katalogu działań odwetowych pozostawiając go jednak otwartym i możliwym do rozszerzenia zadeklarowało 34% badanych firm, z kolei 66% organizacji postawiło na wskazanie ogólnej definicji działań, które mogą zostać uznane za działania odwetowe nie decydując się na budowanie przykładowego katalogu. Należy zwrócić uwagę na fakt, że w obu przypadkach firmy postanowiły zachować elastyczność w zakresie definiowania działań odwetowych i nie ograniczać się jedynie do zachowań jasno wskazanych w treści procedury.

Sposób definiowania działań odwetowych w ramach procedury



Wsparcie w obliczu działań odwetowych

Dyrektywa stanowi, że państwa członkowskie mają zagwarantować sygnalistom odpowiedni poziom wsparcia również poprzez:

a) zapewnienie otwartego dostępu do informacji o prawach sygnalisty, procedurach zgłaszania nieprawidłowości oraz środkach ochrony prawnej przed działaniami odwetowymi;

b) zapewnienie doradztwa prawnego i pomocy prawnej w postępowaniach karnych i transgranicznych postępowaniach cywilnych;

c) zapewnienie pomocy w kontaktach z organami zaangażowanymi w ochronę przed działaniami odwetowymi (w tym wydającymi zaświadczenie o objęciu ochroną, jeśli instytucję taką przewiduje prawo krajowe.

Dobrą praktyką jest, aby każda organizacja podlegająca obowiązkom prawnym wynikającym z krajowej ustawy dotyczącej ochrony sygnalistów wdrożyła odpowiednie środki techniczne i organizacyjne w celu zapobieganiu lub eliminacji działań odwetewych, takie jak regularne szkolenia, polityki przeciwdziałania mobbingowi i dyskryminacji czy też wyrażone wprost sankcje dyscyplinarne za stosowanie działań odwetowych. Projekt ustawy nie przewiduje takiego obowiązku dla pracodawców.

Ponadto poza wyraźnym, ustanowionym w przepisach prawnych, zakazem prowadzenia działań odwetowych, kluczowe znaczenie ma zapewnienie osobom dokonującym zgłoszenia, które doświadczyły już działań odwetowych, dostępu do środków takich jak opieka psychologiczna. Prawo krajowe powinno także przewidywać obowiązek naprawienia szkody spowodowanej podjęciem działania odwetowego.

Naprawienie szkody może przybrać formę przywrócenia stanu poprzedniego, na przykład w sytuacji zwolnienia, przeniesienia lub degradacji, wstrzymania szkolenia, awansu lub przywrócenia odebranego zezwolenia, licencji lub ponownego zawarcia wypowiedzianej umowy, odszkodowania za szkodę rzeczywistą i utracone korzyści, jak np. utracone w przeszłości zarobki, ale także za przyszłą utratę zarobków, koszty związane z przekwalifikowaniem, odszkodowanie za wszelkie inne szkody, takie jak koszty ochrony prawnej i koszty leczenia oraz zadośćuczynienie za poniesione krzywdy, takie jak lęk, ból czy cierpienie. Niestety projekt ustawy nie adresuje w żaden sposób tematów dotyczących chociażby zadośćuczynienia.

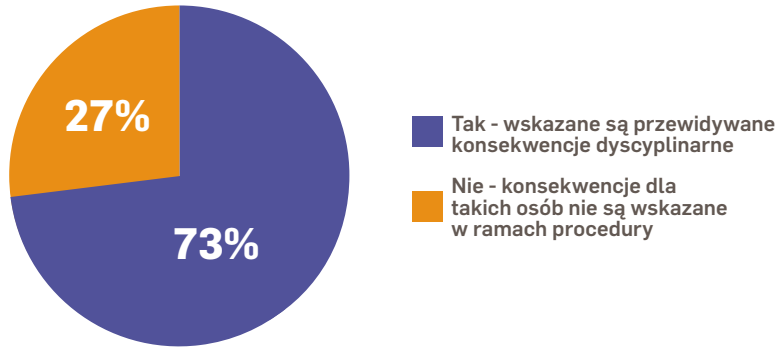
DOBRA PRAKTYKA

W toku rozmów z przedsiębiorcami DZP zidentyfikowało dobrą praktykę, jaką jest zapewnianie pracownikom wsparcia psychologicznego szczególnie potrzebnego w przypadku doznania przez osobę zatrudnioną mobbingu lub dyskryminacji, także na skutek zgłoszenia nieprawidłowości.

Wsparcia takiego może udzielać psycholog zatrudniony przez organizację albo dowolny specjalista wybrany przez pokrzywdzonego, przy zapewnieniu zwrotu sygnaliście poniesionych w związku z tym kosztów. Drugi z prezentowanych modeli zdaje się szczególnie korzystny – sygnalista, który padł ofiarą represji może nie darzyć zaufaniem pracowników w strukturach organizacji.

Zdecydowana większość, bo aż 80% spośród badanych organizacji, przewiduje jasne zasady odpowiedzialności dyscyplinarnej dla tych spośród pracowników, którzy dopuszczają się działań odwetowych względem sygnalistów. Są to konsekwencje podlegające gradacji w oparciu o charakter i wagę działania odwetowego - organizacje deklarują możliwość zastosowania w takiej sytuacji nawet zwolnienia dyscyplinarnego. Procedury 20% badanych firm na chwilę obecną nie przewidują konkretnych konsekwencji dla osób stosujących działania odwetowe.

Wskazanie w ramach procedury przewidywanych konsekwencji dla osób podejmujących działania odwetowe względem sygnalisty



CZEGO POTRZEBUJE BIZNES?

Organizacje, które chcąc promować najwyższe etyczne standardy wdrożyły już rozwiązanie dotyczące ochrony sygnalistów zdają sobie sprawę z wagi marketingu wewnętrznego, szkoleń oraz zapewnienia jak najszerszej ochrony. Aby zapewnić możliwie największą skuteczność systemów w organizacjach, które dopiero będą je budować, ustawodawca mógłby pochylić się nad kwestiami ochrony prawnej lub psychologicznej dla sygnalistów, jak również tematem szkoleń dla pracowników z zakresu wewnętrznych procedur zgłaszania nieprawidłowości - tematy te są poruszane w dyrektywie, zaś polska ustawa w ogóle ich nie dotyka. Wskazanie zakresu, do jakiego pomoc taka powinna być udzielana (działania minimum) mogłoby wspomóc organizację w znalezieniu punktu odniesienia dla wykazania należytej staranności. Bez takiej referencji do przepisów organizacje działają wyłącznie w oparciu o własną intuicję i doświadczenie, nie mając jednak pewności, że ich nawet najlepsze starania w tym obszarze nie zostaną zakwestionowane jako niewystarczające.

12. OCHRONA DANYCH OSOBOWYCH

Prowadzenie systemu whistleblowingowego zarówno w formie elektronicznej jak i papierowej nieodzownie łączy się z przetwarzaniem danych osobowych. Do systemu są wprowadzane informacje o osobie, której dotyczy zgłoszenie, sygnaliście, osobie dotkniętej naruszeniem, a także ewentualnych świadkach. Zbierane w ramach systemów whistleblowingowych informacje w rozumieniu RODO to dane osobowe „zwykłe" (np. imię, informacja o zajmowanym stanowisku, dane kontaktowe) oraz dane osobowe szczególnych kategorii, do których m.in. należą informacje o stanie zdrowia, orientacji seksualnej, poglądach politycznych.

Z uwagi na osobowy charakter informacji znajdujących się w systemie whistleblowingowym, właściciel systemu (który w rozumieniu RODO jest administratorem danych osobowych) powinien przetwarzać je zgodnie z wymaganiami stawianymi przez przepisy RODO. Na konieczność stosowania RODO do ww. danych osobowych zwrócił zresztą wprost uwagę prawodawca unijny w art. 17 Dyrektywy, w którym mowa, że „przetwarzania danych osobowych zgodnie z niniejszą dyrektywą, w tym wymiany lub przekazywania danych osobowych przez właściwe organy, dokonuje się zgodnie z rozporządzeniem (UE) 2016/679 (RODO)". W praktyce oznacza to m.in., że:

- właściciel systemu whistleblowingowego już na etapie projektowania tego systemu powinien uwzględnić ochronę danych osobowych ww. osób (zasada *privacy by design*);
- ochrona danych osobowych powinna być domyślna (zasad *privacy by default*);
- dane osobowe w systemach whistleblowingowych powinny być przetwarzane zgodnie z zasadami z art. 5 RODO, czyli zasadą minimalizacji danych, zasadą legalności, zasadą ograniczonego celu oraz czasu przechowywania danych; a także zasadą integralności, poufności danych;
- osoby, których dane osobowe są przetwarzane powinny otrzymać klauzulę informacyjną z art. 13 albo 14 RODO.

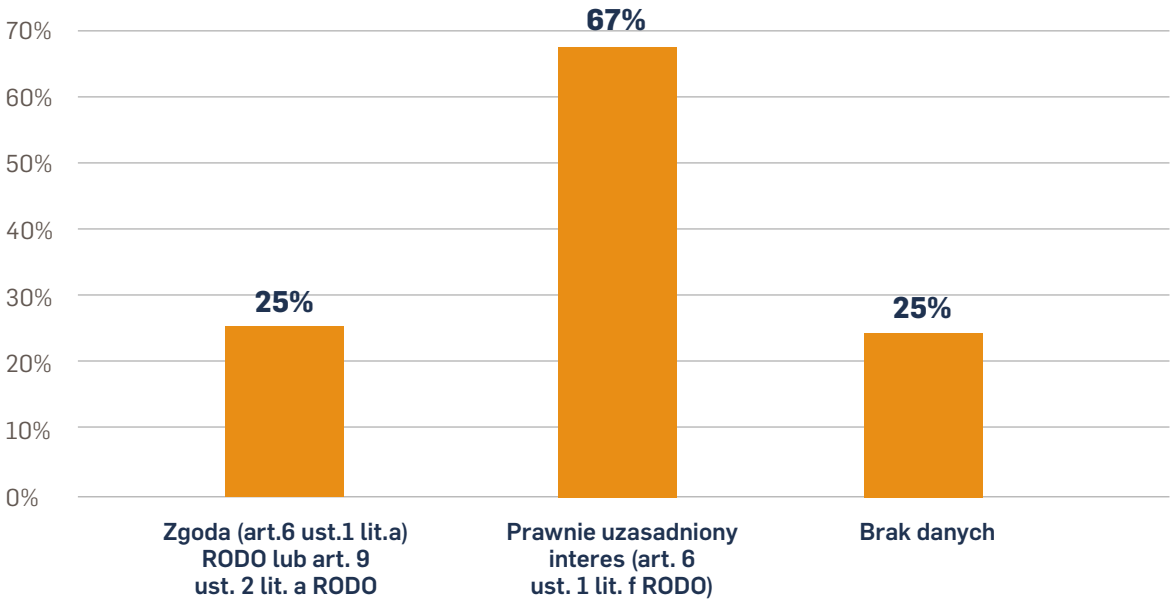
Nie sposób nie zauważyć, że wywiązanie się z ww. obowiązków częściowo pozostaje w sprzeczności z podstawowymi założeniami Dyrektywy. Praktycznie niemożliwe jest zapewnienie poufności, wolności od działań odwetowych sygnaliście, a także zapewnienie ochrony danych i tożsamości uczestnikom postepowania przy jednoczesnym wywiązaniu się z obowiązku podania osobie, której dane są przetwarzane źródła pochodzenia danych osobowych (art. 14 ust. 2 lit. f RODO). W motywie 84 preambuły Dyrektywy, prawodawca unijny wskazał, że „*państwa członkowskie powinny zapewnić skuteczność niniejszej dyrektywy, w tym w stosownych przypadkach poprzez ograniczenie - w drodze aktów prawnych - wykonywania niektórych praw do ochrony danych osobowych osób, których dotyczy zgłoszenie, zgodnie z art. 23 ust. 1 lit. e) i i) oraz art. 23 ust. 2 rozporządzenia* (UE) 2016/679 (RODO), *w zakresie, w jakim i o ile jest to konieczne, by zapobiec i zaradzić próbom utrudniania dokonywania zgłoszeń, utrudniania, udaremniania lub spowalniania działań następczych, w szczególności postępowań wyjaśniających, lub próbom ustalenia tożsamości osób dokonujących zgłoszenia.*" Projekt ustawy przewiduje takie ograniczenie i wyłącza obowiązek z art. 14 ust. 2 lit. f RODO.

Jak ze wskazanymi trudnościami radzi sobie rynek?

W kontekście zasady legalności przetwarzania danych osobowych – organizacje, które brały udział w cyklu sesji dialogowych „Whistleblowing – dobre praktyki etycznego biznesu" najczęściej jako podstawę prawną przetwarzania danych osobowych w ramach systemu whistleblowingowego wskazywały prawnie uzasadniony interes administratora (art. 6 ust. 1 lit. f RODO) - zadeklarowało to 67% organizacji. Zauważyć jednak trzeba, że przywołana podstawa może być wykorzystana tylko i wyłącznie do przetwarzania danych osobowych „zwykłych". Nie może ona natomiast stanowić podstawy prawnej do przetwarzania szczególnych kategorii danych osobowych. W przypadku przetwarzania danych sensytywnych organizacje wskazywały na konieczność uzyskania zgody sygnalisty.

Jeżeli zaś chodzi o wywiązanie się przez administratora z obowiązku poinformowania osoby, której dane osobowe dotyczą (np. osoby, której dotyczy zgłoszenie) o źródle pochodzenia danych osobowych, to ww. firmy wskazały, że co do zasady nie spełniają ww. obowiązku powołując się przy tym na wyjątek z art. 14 ust. 5 lit. b RODO (brak konieczności podania źródła danych z uwagi na to, że jego podanie uniemożliwi lub poważnie utrudni realizację celów takiego przetwarzania). Przyjęte rozwiązanie jakkolwiek zrozumiałe z perspektywy zasady zachowania w poufności danych sygnalisty, nie jest jednak w pełni bezpieczne z perspektywy RODO z uwagi na ocenny charakter przesłanki z art. 14 ust. 5 ust. b RODO. Tym bardziej cieszy wyłączenie obowiązku poinformowania osoby, której dotyczy zgłoszenie o źródle pochodzenia danych.

Podstawa prawna przetwarzania danych osobowych zawartych w zgłoszeniu



Projektowana ustawa, poza wspomnianym wcześniej wyłączeniem obowiązku informowania o źródle danych, przewiduje także maksymalny okres przechowywania danych osobowych jako 5 lat od daty przyjęcia zgłoszenia, co wydaje się być okresem zbyt krótkim mając na uwadze terminy przedawnienia, niektórych spośród naruszeń prawa, których takie zgłoszenia mogą dotyczyć.

Ponadto nakłada także na administratorów systemu obowiązek stosowania rozwiązań technicznych i organizacyjnych zapewniających przechowywanie danych osobowych zgłaszającego oddzielnie od nośnika informacji obejmujących zgłoszenie, co staje się dodatkowym wyzwaniem w kontekście tworzenia wewnętrznych rozwiązań whistleblowingowych.

CZEGO POTRZEBUJE BIZNES?

Kontrowersje budzi wskazany w ustawie maksymalny okres przechowywania danych osobowych. 5 lat od daty przyjęcia zgłoszenia wydaje się być okresem zbyt krótkim, mając na uwadze terminy przedawnienia, niektórych spośród naruszeń prawa, których takie zgłoszenia mogą dotyczyć. Warto, aby w toku procesu legislacyjnego ustawodawca pochylił się nad tym zagadnieniem, ponieważ należy pamiętać, iż niejednokrotnie postępowania wyjaśniające dotyczące niektórych kategorii przestępstw trwają wiele lat i umożliwienie dłuższego przechowywania danych osobowych pozytywnie wpłynęłoby na możliwość komunikacji organizacji z organami ścigania oraz wykazanie należytej staranności w toku działań podjętych celem wyjaśnienia zgłoszenia.

Z punktu widzenia celów funkcjonowania kanałów zgłaszania nieprawidłowości oraz systemu ochrony sygnalistów wydaje się także, że wyłączenie jedynie obowiązku informowania o źródle danych jest niewystarczające. Bardziej zasadne byłoby stworzenie możliwości, w szczególnie uzasadnionych przypadkach, całkowitego odstąpienia od (lub możliwie największego odroczenia realizacji) obowiązku informacyjnego względem osoby, której dotyczy zgłoszenie dla zapewnienia efektywności postępowania.

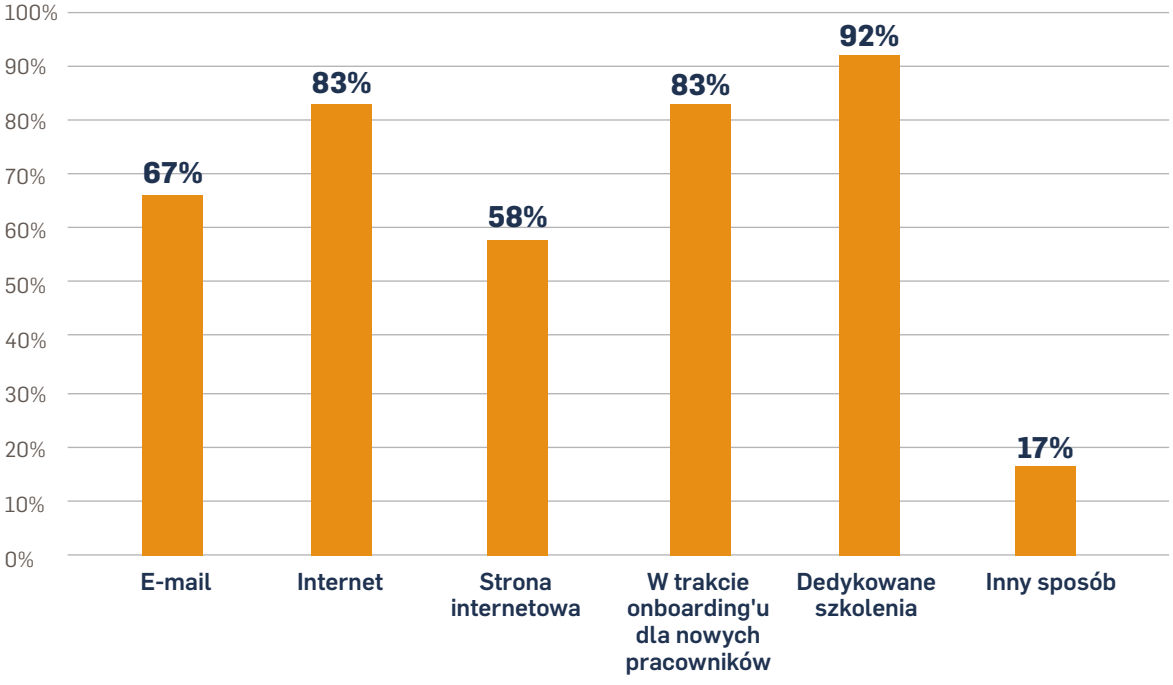
13. SZKOLENIA

Jak wynika z art. 12 ust. 4 i 5 Dyrektywy, osoby wyznaczone, które są odpowiedzialne za przekazywanie wszystkim zainteresowanym osobom informacji na temat procedur dokonywania zgłoszeń, przyjmowanie zgłoszeń i podejmowanie działań następczych w związku ze zgłoszeniami oraz za utrzymywanie kontaktu z sygnalistom - powinny być specjalnie przeszkolone z zakresu rozpatrywania zgłoszeń. Celem takiego szkolenia ma być zapewnienie komunikacji z osobą dokonującą zgłoszenia, a także prowadzenia we właściwy sposób działań następczych w związku ze zgłoszeniem. Natomiast projekt ustawy w obecnym kształcie nie przewiduje obowiązku przeprowadzania szkoleń w zakresie ochrony sygnalistów.

W Dyrektywie ani w projekcie ustawy, nie ma również obowiązku przeprowadzenia szkoleń dla potencjalnych sygnalistów. Unijny ustawodawca wyjaśnia, że osoby, które rozważają zgłoszenie naruszeń prawa Unii, powinny mieć możliwość podjęcia świadomej decyzji o tym, czy, jak i kiedy dokonać zgłoszenia. Z tego powodu podmioty, które ustanowiły wewnętrzne procedury dotyczące whistleblowingu, powinny być zobowiązanie do udzielania informacji na temat tych procedur, a także na temat zewnętrznych procedur dokonywania zgłoszeń do odpowiednich właściwych organów - w sposób zrozumiały i łatwo dostępny. Przykładem, zdaniem unijnego ustawodawcy są informacje umieszczane w widocznym miejscu dostępnym dla wszystkich takich osób oraz na stronie internetowej podmiotu, a także uwzględniane w programach kursów i szkoleń na temat etyki i uczciwości.

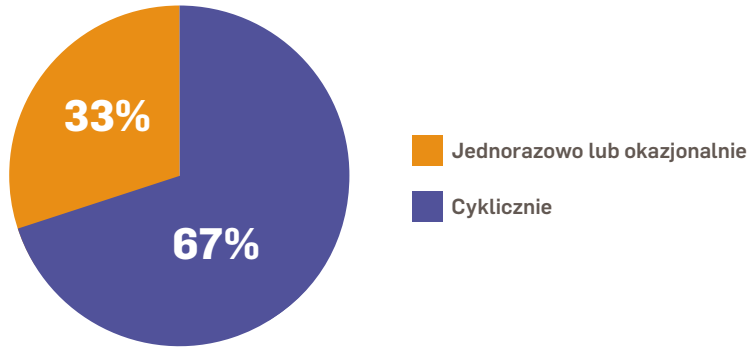
Najpopularniejszą wśród ankietowanych metodą komunikowania sposobu zgłaszania nieprawidłowości okazały się dedykowane szkolenia - ten sposób komunikacji wskazało aż 92% ankietowanych. 83% badanych zadeklarowało, że przekazuje te informacje w trakcie onboardingu nowych pracowników oraz w intranecie.

Sposób/miejsce komunikowania możliwości zgłaszania nieprawidłowości w organizacji



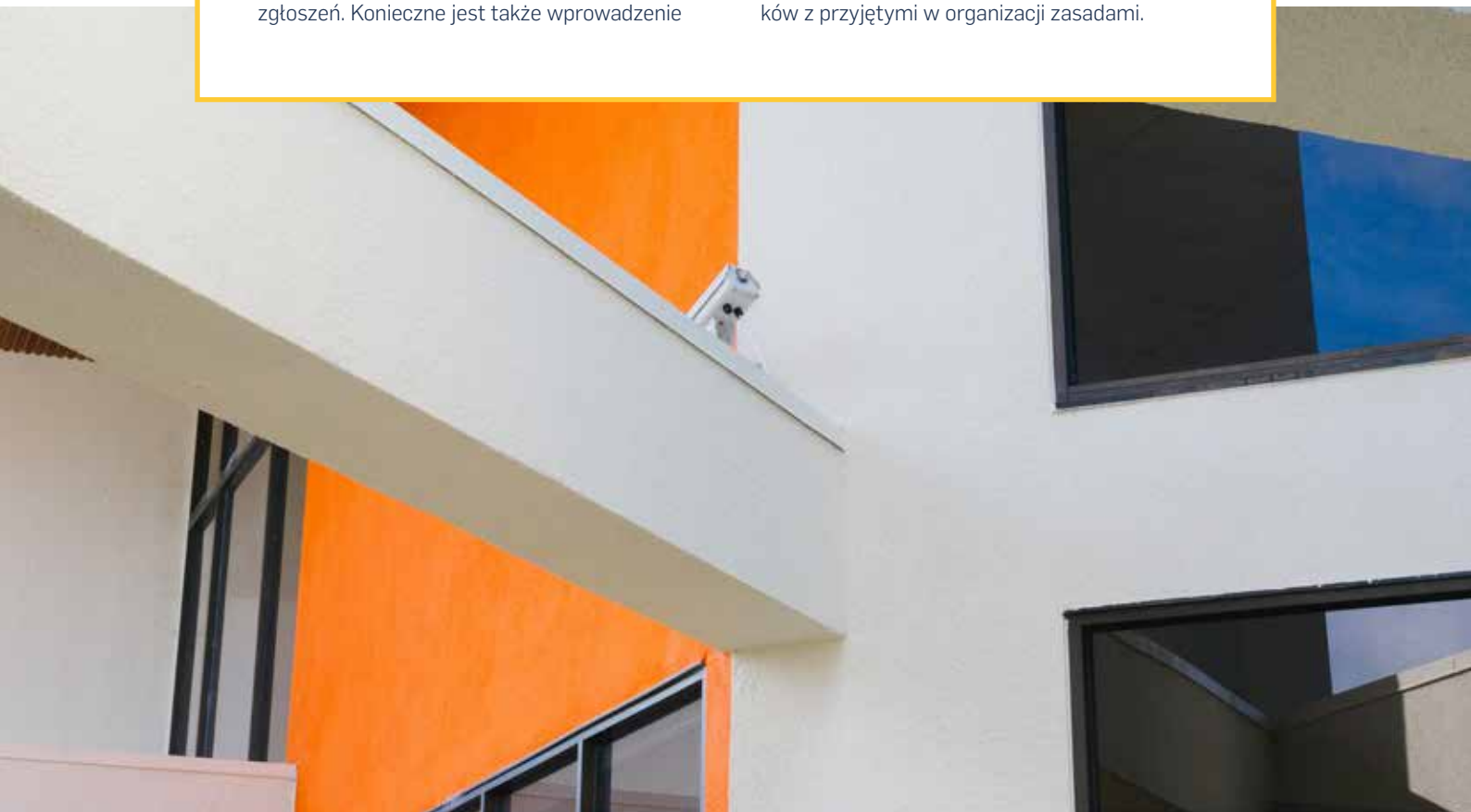
Z kolei 67% ankietowanych zadeklarowało, że komunikację tą prowadzi cyklicznie, a 33% - że incydentalnie lub jednorazowo. Pierwsze z wskazanych rozwiązań znacznie bardziej korzystnie wpływa na kształtowanie kultury speak-up oraz znajomość procedur wśród pracowników.

Częstotliwość komunikowania możliwości zgłaszania nieprawidłowości



CZEGO POTRZEBUJE BIZNES?

Poza obowiązkowymi szkoleniami dla osób odpowiedzialnych za rozpatrywanie zgłoszeń, który to obowiązek wynika z Dyrektywy, polski ustawodawca powinien również uregulować kwestię prowadzenia szkoleń wewnętrznych dla potencjalnych sygnalistów jako metodę komunikowania sposobu zgłaszania nieprawidłowości. W polskiej regulacji prawnej ważne jest również szczegółowe wskazanie zakresu przedmiotowego szkoleń wewnętrznych, zarówno dla potencjalnych sygnalistów jak i dla osób wyznaczonych do rozpatrywania zgłoszeń. Konieczne jest także wprowadzenie obowiązku szkolenia m.in. w zakresie ochrony danych osobowych, przeciwdziałania działaniom odwetowym wobec sygnalisty. W polskiej ustawie powinien znaleźć się również obowiązek dokumentowania szkoleń dla celów dowodowych. Dzięki temu, podmioty obowiązane do ich przeprowadzenia będą mogły wykazać fakt spełnienia obowiązku przeprowadzenia szkolenia oraz podjęcia podczas szkolenia wymaganych kwestii merytorycznych. Bazowanie na punkcie ustawowym odniesienia byłoby prostsze dla wykazania efektywnego zaznajomienia pracowników z przyjętymi w organizacji zasadami.



14. SYSTEM PROCEDUR WEWNĘTRZNYCH DOTYCZĄCYCH WHISTLEBLOWINGU

Zgodnie z projektem ustawy, do wdrożenia regulaminu zgłoszeń wewnętrznych, określającego wewnętrzną procedurę zgłaszania naruszeń prawa i podejmowania działań następczych obowiązani będą pracodawcy zatrudniający co najmniej 50 pracowników. Pracodawca zatrudniający mniej niż 50 pracowników również może ustalić regulamin zgłoszeń wewnętrznych, ale nie jest do tego prawnie zobowiązany.

Taki regulamin zgłoszeń wewnętrznych pracodawca jest zobowiązany ustalić po konsultacji z zakładową organizacją związkową albo przedstawicielami pracowników, którzy zostali wyłonieni w trybie przyjętym u danego pracodawcy – jeżeli u pracodawcy takiego nie działa zakładowa organizacja związkowa.

Omawiany regulamin wchodzi w życie po upływie 2 tygodni od dnia podania go do wiadomości pracowników w sposób przyjęty u danego pracodawcy. Pracodawca jest obowiązany zapoznać pracownika z treścią regulaminu zgłoszeń wewnętrznych przed dopuszczeniem go do pracy.

Jakie informacje muszą znaleźć się w procedurach wewnętrznych?

Dyrektywa precyzuje, że procedury wewnętrzne dotyczące zgłaszania nieprawidłowości i podejmowania działań następczych powinny regulować następujące kwestie:

(a) kanały przyjmowania zgłoszeń zaprojektowane, ustanowione i obsługiwane w bezpieczny sposób zapewniający ochronę poufności tożsamości sygnalisty i osoby trzeciej wymienionej w zgłoszeniu oraz uniemożliwiający uzyskanie do nich dostępu osobom nieupoważnionym – kanały te muszą umożliwiać dokonywanie zgłoszeń na piśmie lub ustnie (np. telefonicznie);

(b) potwierdzenie sygnaliście przyjęcia zgłoszenia w terminie 7 dni od jego otrzymania;

(c) wyznaczenie bezstronnej osoby lub jednostki do podejmowania działań następczych w związku ze zgłoszeniami - może to być ta sama osoba lub ten sam wydział, które przyjmują zgłoszenia, które będą komunikować się z sygnalistą i w stosownych przypadkach zwracać się do sygnalisty o dalsze informacje oraz przekazywać mu informacje zwrotne;

(d) podejmowanie z zachowaniem należytej staranności działań następczych przez wyznaczoną do tego osobę lub jednostkę, również w odniesieniu do zgłoszeń anonimowych - jeśli jest to prawnie przewidziane;

(e) rozsądny termin na przekazanie informacji zwrotnych, nieprzekraczający 3 miesięcy od potwierdzenia otrzymania zgłoszenia lub, w przypadku niewysłania potwierdzenia do sygnalisty - 3 miesięcy od upływu 7 dni od dokonania zgłoszenia;

(f) zapewnienie zrozumiałych i łatwo dostępnych informacji na temat procedur na potrzeby dokonywania zgłoszeń zewnętrznych do właściwych organów i instytucji, organów lub jednostek organizacyjnych Unii Europejskiej.

Zgodnie z projektem ustawy natomiast, regulamin zgłoszeń wewnętrznych powinien określać w szczególności:

1. sposoby przekazywania zgłoszeń,

2. informację, czy wewnętrzna procedura obejmuje przyjmowanie zgłoszeń anonimowych,

3. niezależny organizacyjnie podmiot, który ma prawo przyjmować zgłoszenia i podejmować działania następcze, włączając w to weryfikację zgłoszenia i dalszą komunikację z sygnalistą, w tym występowanie o dodatkowe informacje i przekazywanie sygnaliście informacji zwrotnej - rolę tę może pełnić jeden podmiot upoważniony,

4. obowiązek potwierdzenia przyjęcia zgłoszenia w terminie 7 dni od dnia jego otrzymania, chyba że sygnalista nie podał adresu, na który należy przekazać potwierdzenie,

5. obowiązek podjęcia, z zachowaniem należytej staranności, działań następczych przez upoważniony podmiot,

6. działania następcze podejmowane przez pracodawcę w celu zweryfikowania informacji o nieprawidłowościach oraz środki, jakie mogą zostać zastosowane w przypadku stwierdzenia nieprawidłowości,

7. maksymalny termin na przekazanie sygnaliście informacji zwrotnej, nieprzekraczający 3 miesięcy od potwierdzenia przyjęcia zgłoszenia lub, w przypadku nieprzekazania potwierdzenia sygnaliście, 3 miesięcy od upływu 7 dni od dokonania zgłoszenia,

8. zrozumiałe i jednoznaczne informacje na temat trybu dokonywania zgłoszeń zewnętrznych do organów publicznych oraz, w stosownych przypadkach, do instytucji, organów lub jednostek organizacyjnych Unii Europejskiej.

W projekcie ustawy ustawodawca wskazuje również, że regulamin zgłoszeń wewnętrznych może dodatkowo obejmować również:

1. wyszczególnienie innych niż pracownicy osób, od których przyjmowane są zgłoszenia zgodnie z regulaminem zgłoszeń wewnętrznych, takich jak: byli pracownicy, osoby świadczące pracę na rzecz pracodawcy na innej podstawie niż stosunek pracy, akcjonariusze, wspólnicy, członkowie organu zarządzającego lub organu nadzoru, wolontariusze, stażyści oraz osoby pracujące pod nadzorem i kierownictwem wykonawcy, podwykonawcy i dostawcy,

2. wyszczególnienie innych niż wskazane w projekcie ustawy rodzajów nieprawidłowości, jeżeli pracodawca ustanowi ich zgłaszanie,

3. wyszczególnienie czynników ryzyka odpowiadających profilowi działalności pracodawcy, które sprzyjają nieprawidłowościom stanowiącym naruszenie prawa, np. naruszeniu obowiązków regulacyjnych lub obarczonych ryzykiem korupcji,

4. wyszczególnienie rodzajów nieprawidłowości, które powinny być skierowane w pierwszej kolejności do pracodawcy z wykorzystaniem procedury przewidzianej w regulaminie zgłoszeń wewnętrznych, mogą to być np. naruszenie prawa lub ryzyko korupcji,

5. informację, że zgłoszenie może w każdym przypadku nastąpić również do organu publicznego lub organu centralnego z pominięciem procedury przewidzianej w regulaminie zgłoszeń wewnętrznych, w szczególności, gdy:

a. w regulaminowym terminie na przekazanie informacji zwrotnej pracodawca nie podejmie działań następczych lub nie przekaże sygnaliście informacji zwrotnej lub

b. sygnalista ma uzasadnione podstawy by sądzić, że nieprawidłowość może stanowić bezpośrednie lub oczywiste zagrożenie dla interesu publicznego, w szczególności istnieje ryzyko nieodwracalnej szkody, lub

c. dokonanie zgłoszenia wewnętrznego narazi zgłaszającego na działania odwetowe, lub

d. w przypadku dokonania zgłoszenia wewnętrznego istnieje niewielkie prawdopodobieństwo skutecznego przeciwdziałania nieprawidłowościom przez pracodawcę z uwagi na szczególne okoliczności sprawy, np. możliwość ukrycia, zniszczenia dowodów, istnienia zmowy między pracodawcą a sprawcą naruszenia prawa lub udziału pracodawcy w naruszeniu prawa.

Jak powinien wyglądać system procedur wewnętrznych?

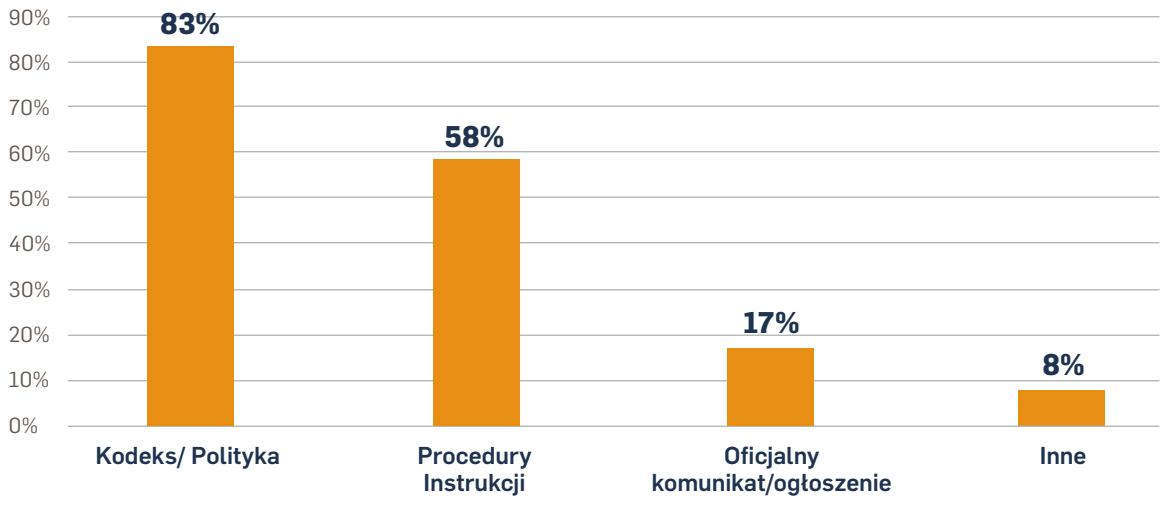
W związku z taką regulacją zasadne jest rozdzielenie tej materii na dwa rodzaje procedur wewnętrznych, skierowanych do różnych adresatów tj. na procedurę informującą o zasadach dokonywania zgłoszeń wewnętrznych, ustanowionych kanałach i wyznaczonych osobach, kierowaną do potencjalnych sygnalistów, oraz na procedurę postępowania ze zgłoszeniami, w której uregulowane zostaną obowiązki przekazania wymaganych informacji sygnaliście, sposób postępowania ze zgłoszeniem i etapy prowadzenia postępowania wyjaśniającego, kierowaną do dedykowanych osób w organizacji. Dzięki takiemu rozwiązaniu możliwe będzie spełnienie różnych potrzeb tych adresatów.

W uwagi na powyższe, w przypadku, gdy w organizacji zostały już sporządzone procedury w zakresie ochrony sygnalistów, po wejściu w życie projektu ustawy, konieczna będzie ich weryfikacja pod kątem obowiązujących przepisów prawnych w tym zakresie.

Ankietowani w badaniu DZP i UNGC wskazywali, że wdrażają wewnętrznie różnego rodzaju regulacje prawne,

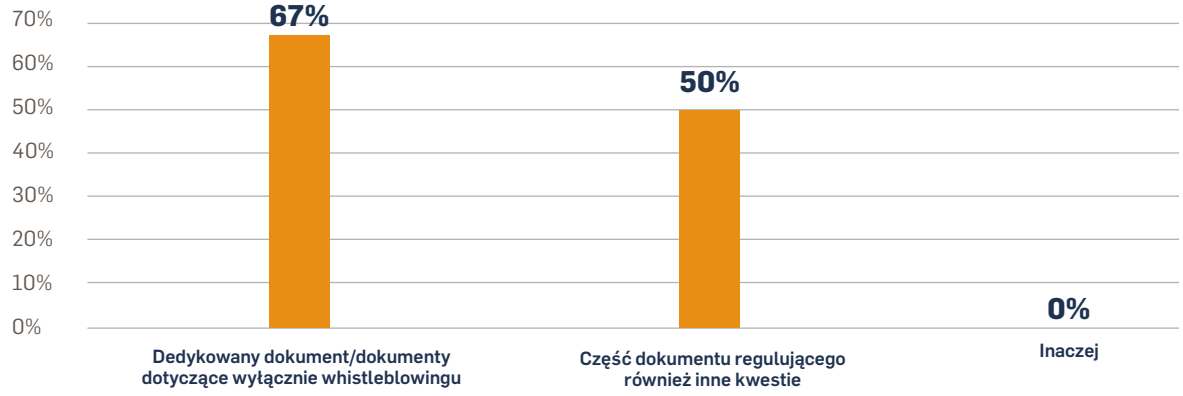
które mają zapewnić ochronę sygnalistom – kwestie whistleblowingu regulują zarówno na gruncie Kodeksu etyki, jak i procedur i instrukcji wewnętrznych.

Rodzaj dokumentu opisującego proces zgłaszania lub rozpatrywania nieprawidłowości



Ponadto aż 67 % wskazało, że kwestie związane z rozpatrywaniem zgłoszeń i prowadzeniem działań wyjaśniających regulują w odrębnym dokumencie.

Forma regulowania procesu zgłaszania i rozpatrywania nieprawidłowości



CZEGO POTRZEBUJE BIZNES?

Polska ustawa implementująca Dyrektywę powinna uwzględnić obowiązek podziału procedur wewnętrznych na dwa rodzaje, ze względu na odmiennych adresatów tj.

- procedury dotyczące zasad zgłaszania nieprawidłowości za pośrednictwem kanałów wewnętrznych - kierowane do potencjalnych sygnalistów, oraz

- procedury dotyczące sposobu postępowania ze zgłoszeniem i prowadzenia działań naprawczych - kierowane do osób zaangażowanych w rozpatrywanie zgłoszeń i prowadzenie postępowań wyjaśniających.

W procedurach kierowanych do sygnalistów powinny znaleźć się głównie postanowienia o charakterze edukacyjnym i zasady zgłaszania, które zapewnią sygnaliście bezpieczeństwo, a w procedurze postępowania ze zgłoszeniem powinny znaleźć się bardziej szczegółowe zasady postępowania ze zgłoszeniem - tj. wyboru osób zaangażowanych, kontaktu z sygnalistą i ochrony poufności w toku postępowania. Zbyt długie regulaminy ograniczają przejrzystość i zrozumiałość takiego dokumentu z perspektywy pracownika, co stanowi także swoiste ryzyko dla organizacji.

15. KULTURA SPEAK UP

Badania pokazują, że poza obawą przed działaniami odwetowymi, tym co zniechęca potencjalnych sygnalistów od zgłoszenia nieprawidłowości, jest przekonanie, że nie odniesie to żadnego skutku oraz nie spotka się z reakcją kierownictwa. Dla efektywnego funkcjonowania systemu whistleblowing nie wystarczy wdrożenie procedur i zapewnienie wolności od represji – trzeba również budować świadomość pracowników i kłaść nacisk na działalność zakorzenioną w wartościach etycznych.

Czym jest kultura Speak Up?

Niczym innym niż kulturą otwartości, uczciwości, odpowiedzialności i wzajemnego zaufania. Speak up culture to nieodzowny element etycznego środowiska pracy – każdy pracownik, niezależnie od zajmowanego stanowiska, powinien mieć przeświadczenie, że jego wysiłki przyczyniają się do tworzenia transparentnej, działającej w zgodzie z przepisami prawa i standardami rynkowymi, organizacji. W konsekwencji, zgłoszenie nieprawidłowości powinno być postrzegane jako element moralnego postępowania oraz działania na rzecz wspólnego dobra.

Ważne, aby pokazywać sygnalistów w pozytywnym świetle, kłaść nacisk na ich rolę w kształtowaniu bezpieczeństwa organizacyjnego i stanąć w zdecydowanej opozycji do mitu sygnalisty-donosiciela.

Co komunikować?

- Nadrzędne wartości organizacji
- Wspólną odpowiedzialność za środowisko pracy
- Treść procedur
- Pozytywne postrzeganie sygnalistów, zgłoszeń i ich znaczenie dla bezpieczeństwa organizacji
- Fakt, że każde zgłoszenie podlega obiektywnemu rozpatrzeniu przez niezależną osobę/zespół

Jak komunikować?

Istnieją rozmaite sposoby komunikowania wartości i sposobów zgłaszania nieprawidłowości, takie jak:

- Procedury
- Szkolenia
- Mailing
- Komunikaty w intranecie
- Bezpośrednie rozmowy z pracownikami

Ustawodawca unijny zwraca przy tym uwagę na konieczność przekazywania pracownikom informacji w sposób klarowny przejrzysty - (art. 9 Dyrektywy precyzuje ten wymóg w szczególności co do sformułowania samych procedur).

DOBRA PRAKTYKA

Narzędziem pomocnym w kształtowaniu kultury speak up oraz przekazywania zasad dotyczących whistleblowingu jest tzw. Legal Design – sztuka formułowania tekstu prawnego i prawniczego w możliwie prosty, przystępny sposób, likwidujący nadmierną formalizację oraz ułatwiający przyswajanie komunikatu poprzez wykorzystanie elementów projektowania graficznego.

Idea ta narodziła się na Uniwersytecie Stanforda i czerpie z założeń user experience, zyskuje coraz szersze uznanie – z elementów Legal Design korzystają między innymi koncerny takie jak Shell, ING, czy PZU. Badania wykazują, że wykorzystanie metodologii pozwala zwiększyć ilość trwale zapamiętywanych przez adresatów dokumentów informacji, a także zminimalizować czas potrzebny na ich przyswojenie.

Dopasowany do potrzeb odbiorców, eliminujący „bezosobowość" przekaz znajduje odzwierciedlenie w zaufaniu pracowników do organizacji oraz zwiększaniu poczucia indywidualnego obowiązku.

Przykład z góry

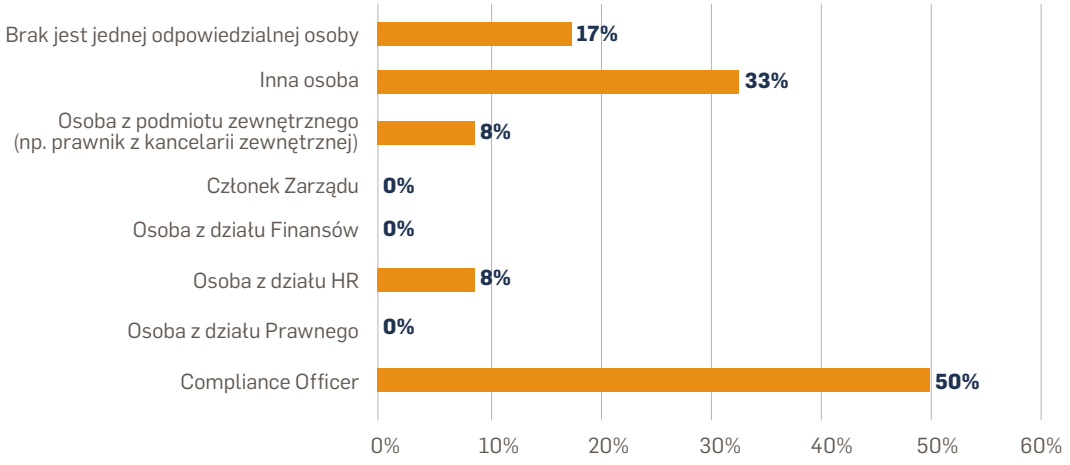
Szczególna odpowiedzialność za kształtowanie kultury speak up spoczywa na kadrze kierowniczej i zarządzającej. To przełożeni powinni dawać swoim podwładnym przykład zaangażowanej i etycznie bezkompromisowej postawy. Nie powinni również pozostawać obojętni na spostrzeżenia i wątpliwości pracowników – ich otwartość bezpośrednio przekłada się na wzajemne zaufanie pracowników różnych szczebli organizacji.

16. POSTĘPOWANIE ZE ZGŁOSZENIEM NIEPRAWIDŁOWOŚCI

Aktualne polskie rozwiązania prawne kreujące obowiązki whistleblowingowe, tj. ustawa AML, Prawo bankowe i Ustawa o ofercie publicznej mają wspólny mianownik - stanowią, bezpośrednio lub pośrednio, że za kwestię przyjmowania zgłoszeń nieprawidłowości powinien odpowiadać członek zarządu (a wyjątkowych przypadkach rady nadzorczej) spółki. Nie oznacza to, że mają oni osobiście przyjmować zgłoszenia. Za ich odbiór odpowiadają najczęściej inni wyznaczeni pracownicy lub komórki organizacyjne – compliance officerowie, pracownicy działów kadr lub prawnych. Zdarza się też, że kompetencje do przyjęcia zgłoszenia są podzielone ze względu na charakter sygnalizowanych naruszeń.

50% ankietowanych w badaniu DZP i UNGC zadeklarowało, że nadzór nad systemem zgłaszania nieprawidłowości w ich organizacji sprawuje compliance officer, 17% - że kompetencja ta jest rozproszona.

Osoby przyjmujące zgłoszenie



Dyrektywa przewiduje, że podmioty zobowiązane powinny wyznaczyć w swojej strukturze konkretną osobę lub komórkę organizacyjną odpowiedzialną za odbiór zgłoszeń - jednakową konstrukcją posłużył się polski ustawodawca w projekcie ustawy.

Postępowanie ze zgłoszeniem

Dobrą praktyką jest podzielenie procesu postępowania ze zgłoszeniem na poziomie procedury. Jako etapy postępowania można wskazać:

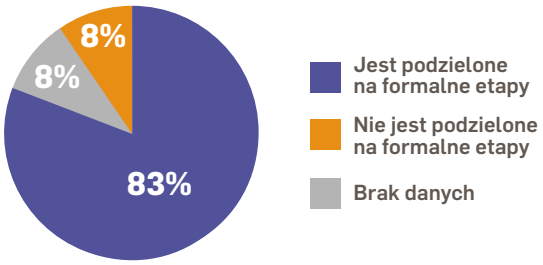
- weryfikację - sprawdzenie zgłoszenia pod względem wymaganych elementów oraz ogólnej zasadności (czy sygnalista podał informacje pozwalające na rozpatrzenie zgłoszenia oraz czy opisana sytuacja stanowi nieprawidłowość);

- wyjaśnienie (tzw. *internal investigation*) - czynności pozwalające na ustalenie czy do nieprawidłowości rzeczywiście doszło. Może ono obejmować działania takie jak rozmowy z personelem, przegląd dokumentacji, korespondencji służbowej pracownika czy nagrań z monitoringu,

- działania naprawcze – wszelkie kroki zmierzające do ograniczenia negatywnych skutków nieprawidłowości oraz uniknięcia wystąpienia podobnej sytuacji w przyszłości - w szczególności weryfikacja procedur wewnętrznych, modyfikacja procesów i edukacja pracowników.

Działania wyjaśniające i naprawcze zawierają się w definicji *działań następczych*, którą posługuje się ustawodawca unijny i krajowy.

Postępowanie ze zgłoszeniem

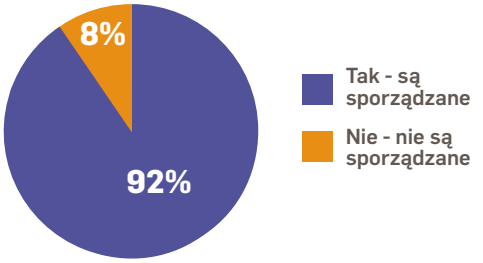


W badaniu DZP i UNGC 83% ankietowanych potwierdziło, że procedury wdrożone w ich organizacji przewidują podział postępowania ze zgłoszeniem na etapy.

Pozytywnie należy też ocenić skrupulatne dokumentowanie postępowania wyjaśniającego. Wszelkie podejmowane czynności (wraz z datą, godziną i uczestnikami) i ich wyniki powinny być opisywane. W konsekwencji powstanie raport pozwalający na odtworzenie przebiegu internal investigation, co będzie w razie potrzeby stanowiło dowód należytej staranności ze strony organizacji.

Innym dobrym nawykiem jest prowadzenie działań naprawczych w oparciu o wcześniej przygotowany plan. Stosowanie takiego rozwiązania zadeklarowało 92% ankietowanych firm. Plan naprawczy powinien mieć charakter rozliczalny, to znaczy wskazywać terminy kolejnych kroków i osoby odpowiedzialne za ich realizację. Decyzja o wszczęciu i czynnościach postępowania naprawczego powinna być podejmowana z uwzględnieniem specyfiki każdego konkretnego przypadku.

Sporządzanie i realizowanie planów naprawczych w związku z wykryciem nieprawidłowości



Zadania w procesie rozpatrywania zgłoszenia - dobre praktyki

Zadania w toku rozpatrywania zgłoszenia i w postępowaniu naprawczym powinny być rozdzielone z uwzględnieniem kompetencji, specyfiki pracy danego pracownika (związku zgłoszenia z obszarem jego specjalizacji) oraz stosownej wiedzy i doświadczenia. W zależności od potrzeb w proces można włączać kolejne osoby. Ważne, żeby zespół wyłoniony w celu wyjaśnienia zgłoszenia mógł działać efektywnie i mieć rzeczywistą możliwość wykonania powierzonych mu zadań.

Projekt ustawy przewiduje, że podmioty zobowiązane powinny wskazać osoby odpowiedzialne za podjęcie działań następczych na poziomie procedury. Nie wydaje się jednak wykluczone, żeby były to podmioty kolegialne, których skład dobierany jest wedle przytoczonych wyżej kryteriów.

CZEGO POTRZEBUJE BIZNES?

Niezwykle istotną, w kontekście zapewnienia należytej ochrony sygnalistów, kwestią jest zapobieganie w ramach rozpatrywania zgłoszenia sytuacji konfliktu interesów. Z procesu przyjęcia i rozpatrywania zgłoszenia oraz wdrażania środków naprawczych muszą być wyłączone osoby, które sygnalista wymienił jako zaangażowane w nieprawidłowość. Zdaniem DZP okoliczność tą należy uwzględnić już na etapie tworzenia procedur dokonywania i wyjaśniania zgłoszeń. Polski ustawodawca z kolei powinien zarządzić ryzykiem związanym z konfliktem interesów w kontekście ochrony sygnalisty na poziomie ogólnym, wprowadzając obowiązek wykluczenia konfliktu interesów podczas wyboru osób rozpatrujących zgłoszenie poprzez wymuszenie posiadania ścieżki alternatywnej, gdy zgłoszenie sygnalisty jako sprawcę identyfikuje osobę co do zasady zaangażowaną w odbieranie lub procedowanie zgłoszeń.

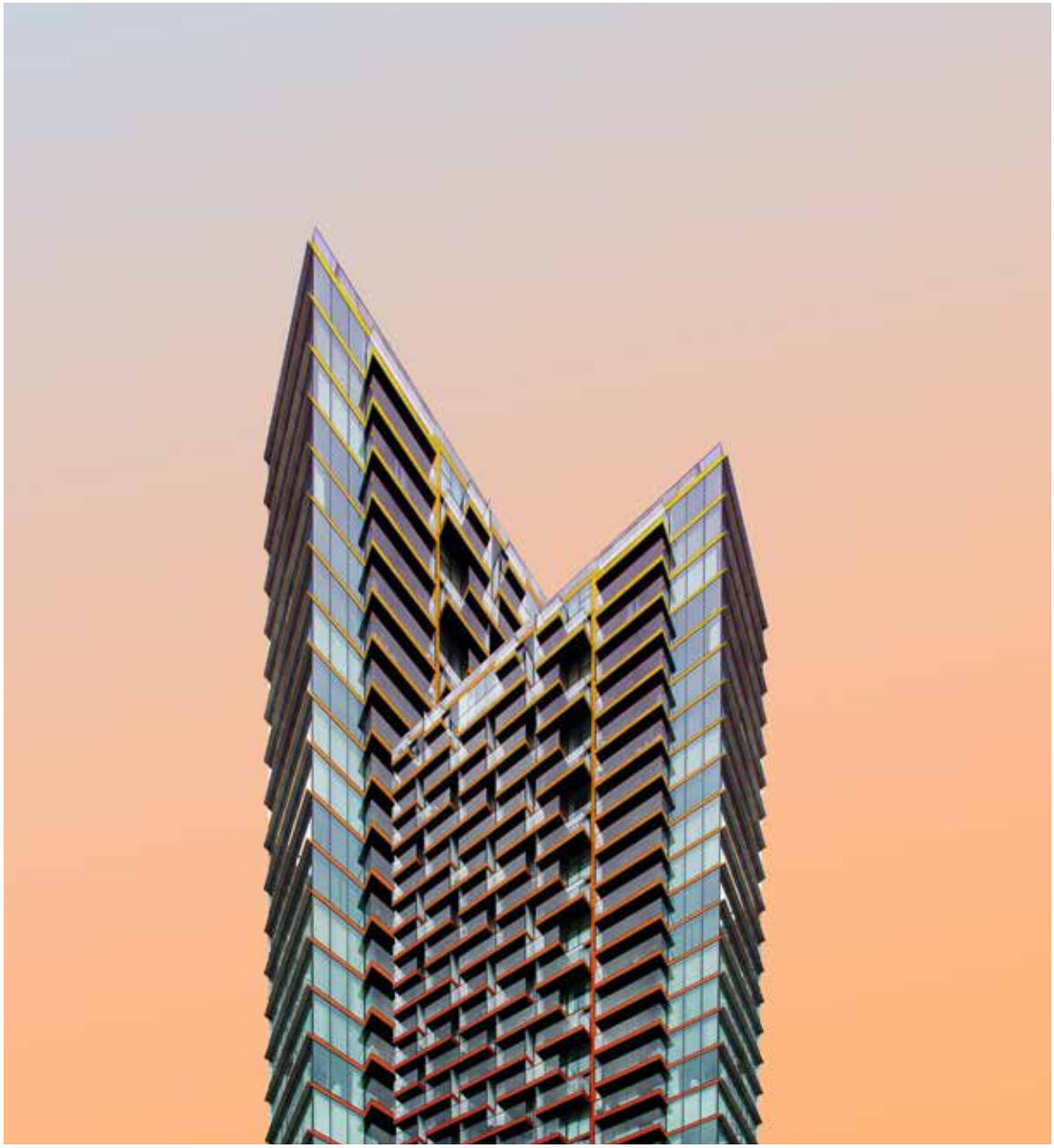
17. REJESTR ZGŁOSZEŃ

Jakie dane przechowywać w rejestrze?

Prowadzenie rejestru wszystkich przyjętych zgłoszeń to obowiązek wynikający z art. 18 Dyrektywy oraz art. 34 projektu ustawy. Co ciekawe obie te regulacje są od siebie znaczącą różne.

W pierwszej kolejności Dyrektywa wymaga prowadzenia rejestru samych zgłoszeń, a nie podjętych w ich wyniku działań następczych, a ustawa wręcz przeciwnie. Projekt wymaga prowadzenia rejestru, który nie zawiera zgłoszeń, a wyłącznie:

1. numer sprawy;
2. przedmiot naruszenia;
3. datę dokonania zgłoszenia wewnętrznego;
4. informację o podjętych działaniach następczych;
5. datę zakończenia sprawy.



Istotne pozostaje pytanie, czy katalog ten jest katalogiem zamkniętym, ponieważ ustawodawca nie posługuje się pojęciem „co najmniej" czy „w szczególności" wymieniając dane jakie musi zawierać rejestr. Taka ścisła interpretacja art. 34 byłaby bardzo szkodliwa, bowiem zakres przechowywanych w rejestrze informacji powinien przede wszystkim umożliwiać odtworzenie biegu sprawy. Stanowi również dowód należytej staranności na potrzeby ewentualnych postępowań prowadzonych przez organy ścigania lub nadzoru. Dokumentowanie całego procesu rozpatrywania zgłoszenia jest istotne dla organizacji właśnie ze względów dowodowych, rejestr powinien zatem zawierać także co najmniej samą treść zgłoszenia.

W jaki sposób przechowywać dane w rejestrze?

Przepisy te są szczególnie mało zrozumiałe w kontekście wymogu art. 30 ust. 3, gdzie zobowiązuje się pracodawcę, aby stosował rozwiązania techniczne i organizacyjne zapewniające przechowywanie danych osobowych zgłaszającego oddzielnie od dokumentu lub innego nośnika informacji obejmujących zgłoszenie. Jakie ma być to miejsce, skoro nie jest nim rejestr? Czy oznacza to też, że ze zgłoszenia pisemnego dane osobowe należy usuwać i przetrzymywać w innym miejscu? Takie działanie wydaje się niecelowe i nieproporcjonalne. Istnieją inne, lepsze metody zapewnienia poufności danych.

Choć większość organizacji prowadzi rejestry w formie elektronicznej, to jednak wciąż można spotkać się z papierowymi postaciami rejestru. Każda z form ma swoje wady i zalety:

• **forma elektroniczna** – największym wyzwaniem prowadzenia rejestru w formie elektronicznej jest zachowanie poufności jego zawartości. Należy zwrócić uwagę, by pracownicy IT nie mieli dostępu do zawartych w rejestrze danych, o czym często zapomina się zlecając jego utworzenie. **Dobrą praktyką rynkową jest opatrzenie pliku stanowiącego rejestr silnym hasłem, które jest znane tylko osobom uprawnionym do rozpatrywania zgłoszeń. Taki plik może być wtedy umieszczany w przestrzeni chmurowej, która zapewnia dodatkową historię dostępu, zmian i umożliwia wykonywanie kopii zapasowych.**

Najlepszą praktyką rynkową jest jednak korzystanie ze zautomatyzowanych rejestrów na odpowiednich platformach IT. Rejestry takie z reguły zawierają komplet informacji o sprawie wraz z jej historią, kompleksowo regulują kwestie prywatności, kontroli dostępu i tworzenia kopii zapasowych. Umożliwiają również łatwe wyszukiwanie danych spraw, a nawet mogą generować statystyki dotyczące wszystkich zgłoszeń przydatne do tworzenia raportów dla np. zarządu.

• **Forma papierowa** – choć jest już stosowana stosunkowo rzadko, zapewnia pewniejszą z perspektywy compliance kontrolę dostępu. Jeżeli rejestr przechowywany jest w bezpiecznym miejscu, do którego dostęp mają wyłącznie upoważnieni pracownicy, to co do zasady zapewnia wysoki stopień poufności. Niestety rejestry takie nie są odporne na zniszczenia mechaniczne, a jeżeli zostaną wykradzione, organizacja traci dostęp do całej zawartej w nich wiedzy.

Kto ma mieć dostęp do rejestru?

Sama kwestia dostępu do rejestru jest też szerzej uregulowana w Dyrektywie niż polskiej ustawie. Rejestry prowadzone są najczęściej przez osoby nadzorujące funkcje compliance w organizacji lub dział compliance. Jeżeli powierzamy wprowadzenie danych do rejestru innym osobom zaangażowanym w postępowanie wyjaśniające, trzeba liczyć się z koniecznością utajnienia tej części rejestru, która nie dotyczy rozpatrywanej sprawy.

Polska ustawa jak i Dyrektywa mówi o uniemożliwieniu uzyskania dostępu do informacji objętej zgłoszeniem nieupoważnionym osobom, jednak Dyrektywa doprecyzowuje te kwestie. Zgodnie z aktem Unijnym dane z rejestru mogą być bowiem ujawniane co do zasady wyłącznie w trzech sytuacjach:

- gdy zgodę taką wyrazi sygnalista; lub
- upoważnionym członkom personelu właściwym do przyjmowania zgłoszeń i podejmowania w związku z nimi działań następczych; lub
- gdy takie ujawnienie jest obowiązkiem wynikającym z prawa Unii lub prawa krajowego w kontekście prowadzonych przez organy krajowe postępowań wyjaśniających lub postępowań sądowych, w tym w celu zagwarantowania prawa do obrony przysługującego osobie, której dotyczy zgłoszenie.

Wydaje się, że polski ustawodawca powinien uwzględnić ten przepis Dyrektywy w projekcie ustawy.

Co ze zgłoszeniami ustnymi?

Dodatkowo Dyrektywa mówi, że zgłoszenia ustne (telefoniczne oraz przekazane w bezpośredniej rozmowie) powinny być dokumentowane w jeden z następujących sposobów:

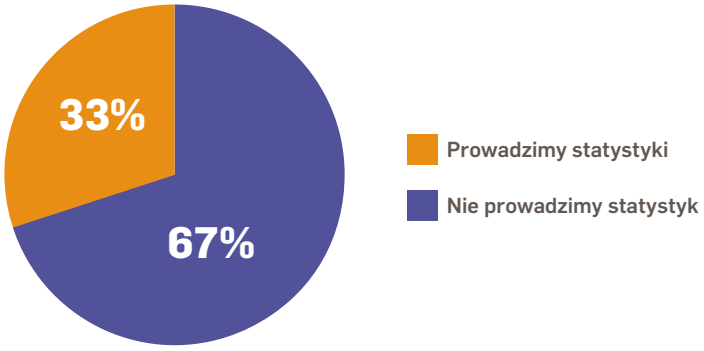
- nagrania rozmowy w formie trwałej i możliwej do wyszukania; lub
- za pomocą kompletnej i dokładnej transkrypcji rozmowy przygotowanej przez członków personelu odpowiedzialnych za rozpatrzenie zgłoszenia; lub
- gdy rozmowa nie jest nagrywana poprzez sporządzenie dokładnego protokołu.

Należy przy tym zapewnić sygnaliście możliwość sprawdzenia, poprawienia i zatwierdzenia transkrypcji rozmowy poprzez jej podpisanie. W ten sam sposób powinno zapewnić się możliwość sprawdzenia, poprawienia i zatwierdzenia sporządzonego protokołu. Projekt ustawy nie transponuje tych przepisów, co również może budzić wątpliwości w przypadku zdecydowania się na założenie linii telefonicznej lub przyjmowania zgłoszeń osobiście.

Dlaczego jeszcze prowadzić rejestr?

Jak wskazuje badanie DZP i UNGC, prowadzenie rejestru pozwala organizacjom na pozyskanie istotnych informacji o funkcjonowaniu systemu whistleblowingowego oraz prowadzenie statystyk. W badaniu ankietowani wskazywali, że gromadzą m.in. informacje o tym jaki procent z uzyskanych zgłoszeń pozwala na ujawnienie rzeczywistej nieprawidłowości, a czasem – jaki procent zgłoszeń dokonywany jest w złej wierze. Badania wykazało, że wśród firm, które prowadzą statystyki, średnio ok. 50-60% zgłoszeń weryfikowanych jest jako prawdziwe.

Prowadzenie statystyk w ramach rejestrów



Jak długo przechowywać dane osobowe?

Wątpliwości może budzić kwestia, jak długo przechowywać dane osobowe w rejestrze, szczególnie że na mocy projektu ustawy pracodawca musi być administratorem tych danych. Tak jak pisaliśmy w rozdziale 12, polska ustawa rozstrzyga tę kwestię w zakresie danych osobowych – wyznaczając limit przechowywania takich danych na 5 lat. Okres ten wydaje się zbyt krótki, biorąc pod uwagę, że podstawowy termin przedawnienia roszczeń cywilnych wynosi 10 lat, a karnych nawet 15 czy 30 lat. Usuwając takie dane osobowe nawet 5 lat przed upływem terminu przedawnienia, narażamy się na brak możliwości wykazania należytej staranności i obrony interesów organizacji w przypadku toczących się kilka lat później postepowań.

CZEGO POTRZEBUJE BIZNES?

Ponieważ przepisy Dyrektywy i projektu ustawy są znacząco różne, przede wszystkim pożądane byłoby ujednolicenie wymagań ustawy do standardu Dyrektywy. W szczególności powinny zostać zaadresowane takie kwestie jak:

ï Oparcie rejestru w pierwszej kolejności na archiwizacji zgłoszeń (zgodnie z wymaganiami Dyrektywy) i dopiero rozbudowanie go o otwarty katalog dodatkowych informacji (tak żeby organizacje mogły w ramach niego prowadzić np. statystyki);

ï Sformułowanie proporcjonalnych wymogów co do technicznych aspektów prowadzenia rejestru (szczególnie że ustawa ma obowiązywać nawet dla organizacji zatrudniających od 50 osób);

ï Utworzenie jasnego katalogu wyjątków w zakresie dostępu do rejestru zgodnego ze standardami Dyrektywy;

ï Ustalenie jasnych zasad dokumentowania zgłoszeń ustnych;

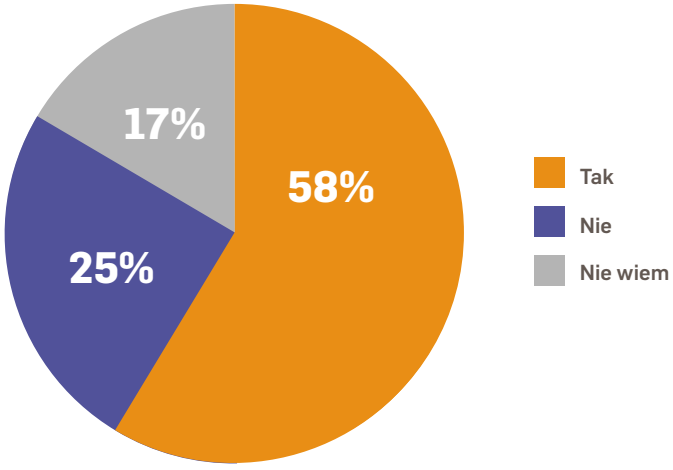
ï Wydłużenie terminów przedawnienia roszczeń, tak by organizacje mogły chronić swoje interesy i wykazywać należytą staranność tak długo, jak w związku z danym naruszeniem mogłaby być do tego zobowiązana.

18. ROLA BENCHMARKÓW W PRZYGOTOWANIU AKTÓW WYKONAWCZYCH

Systemy zgłaszania nieprawidłowości to nie tylko przedmiot zainteresowania prawodawcy, ale też twórców standardów i wytycznych zbierających najlepsze praktyki w danych obszarach.

Aż 58% uczestników badania wskazało, że stosuje w ramach swoich systemów dodatkowe wytyczne, normy lub benchmarki. Najczęściej wymienianymi standardami były norma ISO 37001 oraz wytyczne Giełdy Papierów Wartościowych.

Budowa systemu w oparciu o dodatkowe wytyczne/normy/benchmarki



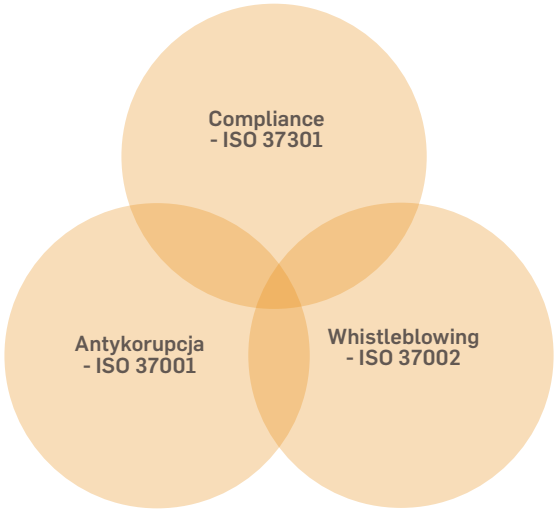
Benchmarki międzynarodowe

Chcąc wskazać najlepsze i najpowszechniej uznawane benchmarki, należy przede wszystkim wymienić normy ISO z zakresu compliance. Istnieją obecnie trzy takie normy:

- ISO 37001:2016 – System zarządzania działaniami antykorupcyjnymi;
- ISO 37301:2021 – Wymagania i wytyczne dla systemów zarządzania zgodnością;
- ISO 37002:2021 – Wytyczne w zakresie zarządzania systemami zgłaszania nieprawidłowości.

Z perspektywy raportu i tematyki whistleblowing najważniejsza jest najnowsza z nich - opublikowana 27 lipca 2021 r. norma 37001 dotycząca stricte systemu zgłaszania nieprawidłowości. Należy jednak zaznaczyć, że także pozostałe normy zawierają określone wymagania w zakresie tworzenia systemów zgłaszania nieprawidłowości.

Norma antykorupcyjna wymaga m.in. umożliwienia anonimowego zgłaszania nieprawidłowości korupcyjnych, zapewnienia odpowiedniego poziomu poufności zgłoszeń i ochrony przed działaniami odwetowymi. Z kolei norma



dla systemów zarządzania zgodnością co prawda jedynie poleca wdrożenie takich kanałów, zwraca jednak uwagę na korzyść z ich posiadania - pozyskiwanie informacji zwrotnych istotnych dla oceny funkcjonowania systemu compliance w organizacji.

Norma whistleblowingowa ustanawia natomiast najlepszy standard rynkowy w zakresie zgłaszania nieprawidłowości. Wyróżnia m.in. 4 etapy procesu whistleblowingowego i zawiera schematy działań podejmowanych w ramach procesu rozpatrywania zgłoszenia. Uwzględnia konieczność oceny kontekstu organizacji, wymogi dotyczące przywództwa dla kadry kierowniczej, zakres procedur, zakres dokumentacji, obowiązek prowadzenia szkoleń, obowiązek oceny jakości systemu i obowiązek doskonalenia systemu. Choć norma 37002 nie jest certyfikowalna, to stosowanie się do jej założeń daje pewność, że zrobiliśmy wszystko co możliwe by stworzyć efektywny system whistleblowing. Nawet jeżeli nie planujemy stworzenia rozwiązania zgodnie z normą, warto się z nią zapoznać, ponieważ podchodzi do kwestii zgłaszania nieprawidłowości w sposób najbardziej kompleksowy.

Normy 37001 i 37301 są certyfikowalne, a ponieważ każda z trzech norm dotyczy podobnej sfery działalności organizacji, warto zatem wdrożyć wszystkie trzy standardy ISO w ramach jednego projektu compliance. Zaletą takiego wdrożenia jest:

- kompleksowa prewencja nadużyć,
- wiarygodność w oczach partnerów biznesowych,
- szeroka ochrona organizacji w świetle rozwijających się regulacji prawnych,
- korzystność finansowa takiego wdrożenia i znacząca oszczędność czasu,
- uzyskanie najlepszego możliwego dowodu należytej staranności w zarządzaniu zabezpieczającym kadrę kierowniczą,
- wyznaczenie trendów na rynku i wyprzedzenie konkurencji.

Benchmarki sektorowe

Oprócz standardów międzynarodowych, często tworzone są również lokalne, sektorowe benchmarki. Przykładem takiego polskiego standardu są „Standardy rekomendowane dla systemu zarządzania zgodnością w zakresie przeciwdziałania korupcji oraz systemu ochrony sygnalistów w spółkach notowanych na rynkach organizowanych przez Giełdę Papierów Wartościowych w Warszawie S.A.". Wskazują one m.in. bardzo szeroki krąg podmiotów, którym powinny być udostępniane anonimowe kanały zgłaszania. Zaleca się bowiem by powołany system sygnalizowania umożliwiał pracownikom, współpracownikom, kontrahentom, partnerom, w tym biznesowym i wszystkim osobom wykonującym jakiekolwiek czynności w imieniu lub na rzecz Spółki przekazywanie informacji w sposób poufny, zapewniający całkowitą anonimowość. Warto zaznaczyć, że w trakcie przygotowywania są także nowe standardy GPW obejmujące swoim zakresem ściśle tematykę whistleblowingu. Są one tworzone jako rekomendacje dla spółek giełdowych w oparciu o brzmienie Dyrektywy oraz zgodne z projektem ustawy.

Na kształt polskich systemów zgłaszania nieprawidłowości często wpływają też wymogi stawiane przed innymi państwami z uwagi na konieczność realizacji standardów korporacyjnych przyjętych przez centralę. Niezależnie od tego jaki standard stosujemy, warto konfrontować go z prawem polskim. Jeśli zachowujemy w tym zakresie zgodność, to umiejętność wskazania standardu będącego podstawą systemu zgłoszeń pozytywnie wpływa na wizerunek i wiarygodność naszej organizacji. Zarówno w oczach kontrahentów jak i nawet organów ścigania lub nadzoru.

PODZIĘKOWANIA

Nasz raport nie mógłby powstać, gdyby nie zaangażowanie i wkład wielu podmiotów zarówno na etapie cyklu sesji dialogowych – poprzez udział w nich i dzielenie się trafnymi wnioskami i spostrzeżeniami oraz wypracowanymi przez organizacje dobrymi praktykami, jak również na etapie przygotowywania raportu – poprzez jego merytoryczne opracowanie oraz odpowiedzi firm na pytania ankietowe w ramach badania rynku.

Nie sposób wymienić wszystkich uczestników sesji dialogowych i firm zaangażowanych w poszczególne rozmowy, obecnych na spotkaniach i udzielających się w dyskusji. Państwa obecność i refleksje wzbogaciły ten raport o praktyczne doświadczenia i potrzeby, które mogliśmy zaadresowa w raporcie.

Serdecznie dziękujemy wszystkim osobom, które wzięły udział w naszych sesjach dialogowych w charakterze prelegentów:

Wojciech Gonciarz
Państwowa Inspekcja Pracy | Dyrektor Departamentu Prawnego

Anna Sekinda-Maicka
Urząd Ochrony Konkurencji i Konsumentów | Zastępca Dyrektora Departamentu Ochrony Konkurencji

Urszula Góral
Urząd Ochrony Danych Osobowych | Dyrektor Departamentu Współpracy Międzynarodowej i Edukacji

Karolina Gierdal
Kampania Przeciw Homofobii | Prawniczka Grupy Prawnej KPH

Beata Gilicińska
Lux Med | Ekspert ds. Systemów Antykorupcyjnych

Marcin Szczepański
Siemens Energy | Compliance Officer for Poland, Czech Rep., Hungary, Slovakia, Turkey, and Ukraine

Anna Tomiczek
Tauron Polska Energia | Kierownik Zespołu Compliance

Grzegorz Procajło
Tauron Polska Energia | Starszy specjalista ds. ochrony danych osobowych

Radosław Lewandowski
Rzecznik Etyki Grupy Kapitałowej PKP Energetyka

Justyna Olszewska
Skanska| Ethics Officer

Robert Sroka
Abris Capital | Dyrektor ds. ESG

Piotr Chmiel
T-Mobile | Dyrektor Departamentu Zarządzania Zgodnością

Helena Zielińska
Uniwersytet Wrocławski

Anna Potocka-Domin
UN Global Compact Network Poland | Członkini Rady Programowej UN Global Compact Network Poland, Dyrektorka Programu Standard Etyki, Wiceprezeska BCC

Kamil Wyszkowski
UN Global Compact Network Poland | Dyrektor Wykonawczy

Jarosław Łukawski
Partner w zespole Prawa Ochrony Konkurencji i Konsumentów DZP

Julia Besz
Associate w zespole Compliance DZP

Sylwester Silski
Associate w zespole Prawa Pracy DZP

Aleksandra Zomerska
Associate w zespole Ochrony Danych Osobowych DZP

Jakub Dydak
Associate w zespole Compliance DZP

Składamy również podziękowania dla partnerów strategicznych raportu za ich patronat i wzbogacenie raportu o wkłady analityczne oparte o szczegółową prezentację własnych doświadczeń compliance w obszarze budowania systemów zgłaszania:

Boehringer Ingelheim sp. z o.o.
Lux Med sp. z o.o.
Oknoplast sp. z o.o.
Siemens Energy sp. z o.o.
Solaris Bus & Coach sp. z o.o.
Tauron Polska Energia S.A.

Szczególny wkład w przeprowadzenie cyklu sesji dialogowych oraz przygotowanie raportu mieli także członkowie Programu Standardu Etyki UN Global Compact Network Poland:

3M
Abris Capital Partners Sp. z o.o.
Allegro.pl Sp. z o.o.
BASF Polska Sp. z o.o.
BNP Paribas Bank Polska S.A.
Crido
Diageo Polska Sp. z o.o.
DOZ S.A.
ENEA S.A.
ING Bank Śląski S.A.
Kulczyk Foundation
L'Oreal Polska Sp. z o.o.
NHOOD Services Poland Sp. zo.o.
PKP Energetyka S.A.
Santander Bank Polska S.A.
Skanska Property Poland Sp. z o.o.
STU ERGO Hestia S.A.
T-MOBILE POLSKA S.A.

GŁOS BIZNESU

SIEMENS energy

OPIS ORGANIZACJI ORAZ FUNKCJONUJĄCEGO SYSTEMU WHISTLEBLOWINGOWEGO:

Siemens Energy Sp. z o.o. jest polską spółką-córką koncernu Siemens Energy AG, wiodącego światowego dostawcy rozwiązań, usług oraz produktów związanych z produkcją, przesyłem oraz zarządzaniem energią.

System whistleblowingowy pod nazwą „Tell-Us" został wdrożony w całym koncernie Siemensa już w 2008 roku w ramach całościowego wdrożenia systemu Compliance w oparciu o standardy FCPA. System ten jest operowany przez zewnętrznego dostawcę, firmę BKMS, co zapewnia anonimowość zgłoszeń, oraz ochronę sygnalistów – Siemens nie posiada bezpośredniego dostępu, otrzymuje jedynie raporty dot. zgłoszeń lub może umieszczać tam (pośrednio, poprzez BKMS) informacje np. do sygnalistów, jeśli sobie tego życzą. Po wydzieleniu Siemens Energy w 2020 roku, system ten przyjął nazwę „Speak-Up", lecz funkcjonalność pozostała taka sama.

Dodatkowo w koncernie Siemens istnieje drugi kanał raportowania nieprawidłowości tj. „Ombudsman", czyli zewnętrzna kancelaria prawna zatrudniana przez Komitet Audytu Rady Nadzorczej koncernu. Celem jest umożliwianie składania zgłoszeń na ew. naruszenia ze strony najwyższych władz koncernu.

KORZYŚCI I WYZWANIA ZWIĄZANE Z FUNKCJONOWANIEM SYSTEMU ZGŁASZANIA NIEPRAWIDŁOWOŚCI:

KORZYŚCI:

- wentyl bezpieczeństwa dla pracowników, którzy mogą dokonać zgłoszeń zauważonych nieprawidłowości w sytuacji, gdy nie chcą / bądź nie mogą pozwolić sobie na zgłoszenie bezpośrednie.
- doskonale źródło informacji dla firmy nt. naruszeń, a co za tym idzie możliwość dokonywania ulepszeń w funkcjonowaniu firmy.

WYZWANIA:

- utrzymanie wśród pracowników przekonania, ze warto sygnalizować naruszenia tj. że jest to we wspólnym interesie wszystkich,. Jest to szczególnie trudne po wielu latach funkcjonowania systemu.

SZCZEGÓLNE OSIĄGNIĘCIA ZWIĄZANE Z SYSTEMEM ZGŁASZANIA NIEPRAWIDŁOWOŚCI:

System działa już ponad 13 lat, co roku rejestrowane są tysiące zgłoszeń w skali całego świata, kilkanaście/kilkadziesiąt w Polsce. System umożliwia składanie zgłoszeń wszystkim i na każdy temat – nie ma tu żadnych ograniczeń. Jednocześnie zapewnia on anonimowość zgłaszającym (Siemens nie ma bezpośredniego dostępu do systemu), ale umożliwia też kontakt z sygnalistami, którzy mogą (pozostając anonimowi) zakładać na tym systemie coś w rodzaju skrzynki kontaktowej.

OCZEKIWANIA WZGLĘDEM USTAWODAWCY W KONTEKŚCIE KSZTAŁTU USTAWY IMPLEMENTUJĄCEJ DYREKTYWĘ O SYGNALISTACH:

Wdrożenie dyrektywy bez niepotrzebnych komplikacji i przesady we wprowadzonych zapisach. Już sama dyrektywa jest fundamentalna zmianą, więc oczekujemy, że lepiej byłoby się skoncentrować na jej wdrożeniu, a ew. zmiany/zaostrzenia rozważać dopiero po zebraniu doświadczeń z jej funkcjonowania. Wdrożenie dyrektyw powinno także wymusić docelowo upowszechnienie się systemów Compliance w podmiotach, które dotychczas takich systemów nie posiadały. A te, które już posiadają powinny zmierzać w kierunku systemów efektywnych (wdrożonych na poważnie), a unikać tzw. „window dressing".

UDANE I PROBLEMATYCZNE KWESTIE ZWIĄZANE Z SYSTEMEM ZGŁASZANIA NIEPRAWIDŁOWOŚCI:

Można powiedzieć, że sam system zgłaszania działa bez zarzutu. Wyzwaniem bywają same postępowania wyjaśniające, które czasem zajmują zbyt dużo czasu głównie z uwagi na szczupłość zasobów przeznaczonych do tego celu.

Obserwacje pokazują, że absolutna większość zgłoszeń poprzez system whistleblowingowy (o ile nie prawie wszystkie), są to zgłoszenia anonimowe. Natomiast zgłoszenia pod nazwiskiem dokonywane są bezpośrednio do Compliance Officerów (najczęściej, czasem do HR lub Zarządu).

Generalnie najważniejsze jest, żeby zgłoszenia napływały bez względu na formę, sposób czy miejsce zgłoszenia. Wtórne jest, czy będzie to zawansowany system internetowy, czy metody tradycyjne (np. anonimowe, papierowe listy). A zgłoszenia będą napływały tylko wtedy, gdy interesariusze będą przekonani, że zgłoszenia są rozpatrywane, wyjaśniane i w przypadku ich potwierdzenia wyciągane są konsekwencje.

Natomiast nawet najlepszy system nic nie da, gdy kierownictwo działa selektywnie i np. surowo ukarze szeregowego pracownika, który został złapany na wynoszeniu papieru do drukarki, a „ukręci łeb" sprawie związanej z prawdziwymi malwersacjami, ale w którą jest zamieszany wysoko postawiony członek kierownictwa.

NAJCIEKAWSZA HISTORIA ZWIĄZANA Z SYSTEMEM WHISTLEBLOWING:

W całej mojej karierze Compliance Officera, zarówno w Polsce jak i zagranicą nie spotkałem się nigdy ze zgłoszeniem, które było całkowicie nieprawdziwie (w domyśle, „dokonane w złej wierze"). Każde, nawet najbardziej lakoniczne czy napisane w niegramatyczny sposób zawierało w sobie ziarno prawdy i w ogromnej większości wskazywało na rzeczywiste naruszenia.

GRUPA LUXMED

OPIS ORGANIZACJI ORAZ FUNKCJONUJĄCEGO SYSTEMU WHISTLEBLOWINGOWEGO:

Grupa Lux Med to największa prywatna sieć medyczna w Polsce, oferujące kompleksową opiekę medyczną i ubezpieczenia zdrowotne. Grupa Lux Med jest częścią międzynarodowej grupy Bupa.

W grupie Lux Med funkcjonuje centralny system zgłaszania nieprawidłowości, który jest obsługiwany przez zewnętrznego dostawcę. Wśród dostępnych kanałów zgłoszeń są: infolinia, platforma on-line oraz lokalnie dedykowany mejl, zgłoszenia do bezpośrednio przełożonego czy do Speak Up oficera. Zgłoszenia mogą być dokonywane anonimowo lub imiennie i są obsługiwane przez dedykowany zespół. Dokumenty dotyczące zgłoszeń są archiwizowane w centralnym systemie, dostęp do którego mają ściśle określone osoby, które prowadzą postępowanie, Informacja zwrotna jest przekazywana. Zgłaszającemu po zakończeniu postępowania. System whistleblowing jest opisany w procedurze Speak Up, która jest dostępna dla pracowników i współpracowników w intranecie.

KORZYŚCI I WYZWANIA ZWIĄZANE Z FUNKCJONOWANIEM SYSTEMU ZGŁASZANIA NIEPRAWIDŁOWOŚCI:

Wśród korzyści należy wymienić transparentność i zapewnienie otwartej komunikacji z pracownikami i współpracownikami. Dzięki systemowi whistleblowingu firma ma możliwość powzięcia informacji o potencjalnych nieprawidłowościach na wczesnym etapie i dzięki temu może szybko reagować i wprowadzać odpowiednie kroki naprawcze.

SZCZEGÓLNE OSIĄGNIĘCIA ZWIĄZANE Z SYSTEMEM ZGŁASZANIA NIEPRAWIDŁOWOŚCI:

Jednym z największych osiągnięć jest podniesienie świadomości wśród pracowników na temat etyki w biznesie, zbudowanie atmosfery zaufania i kultury wsłuchiwania się w głos pracowników. Udało się również aktywniej włączyć pracowników w dbałość o dobro wspólne jak i uczynić ich odpowiedzialnym za nie m.in. poprzez zwracanie uwagi na wszelkie naruszenia czy nieprawidłowości.

UDANE I PROBLEMATYCZNE KWESTIE ZWIĄZANE Z SYSTEMEM ZGŁASZANIA NIEPRAWIDŁOWOŚCI:

Samo dokonywanie zgłoszeń oraz ich wstępna weryfikacja udaje się dobrze jak i przypisanie zgłoszeń do poszczególnych zespołów prowadzących postępowania wyjaśniające. Problemem jest zapewnienie jednolitego standardu dokumentowania zgłoszeń i czynności podejmowanych w toku postępowania wyjaśniającego jak również terminowość prowadzenia postępowań wyjaśniających i wdrażania działań naprawczych.

OCZEKIWANIA WZGLĘDEM USTAWODAWCY W KONTEKŚCIE KSZTAŁTU USTAWY IMPLEMENTUJĄCEJ DYREKTYWĘ O SYGNALISTACH:

Szczegółowe uregulowanie kwestii przetwarzania danych osobowych na wszystkich etapach postępowania w tym określenie czasu retencji danych, rozstrzygnięcia czy grupy kapitałowe mogą korzystać z centralnego systemu i na jakich zasadach.

OPIS ORGANIZACJI ORAZ FUNKCJONUJĄCEGO SYSTEMU WHISTLEBLOWINGOWEGO:

Spółka działa w branży produkcji motoryzacyjnej, zatrudnia ok. 2400 osób, wchodzi w skład międzynarodowej grupy kapitałowej jako spółka matka oraz spółka córka. Aktualnie działający system whistleblowingowy w spółce jest systemem na poziomie grupy kapitałowej, jednak intensywnie pracujemy nad wdrożeniem systemu dedykowanego dla naszej spółki.

KORZYŚCI I WYZWANIA ZWIĄZANE Z FUNKCJONOWANIEM SYSTEMU ZGŁASZANIA NIEPRAWIDŁOWOŚCI:

Mamy nadzieję, że uda nam się zbudować transparentny, zbalansowany i prężnie działający system, który realnie wpłynie na wykrywanie nieprawidłowości, co z kolei pozwoli na podjęcie odpowiednich działań zapobiegawczych na przyszłość.

OCZEKIWANIA WZGLĘDEM USTAWODAWCY W KONTEKŚCIE KSZTAŁTU USTAWY IMPLEMENTUJĄCEJ DYREKTYWĘ O SYGNALISTACH:

Oczekujemy, że regulacje wprowadzone przez ustawodawcę pozwolą na zbudowanie zbalansowanych systemów whistleblowingowych, które z jednej strony pozwolą na wykrywanie nieprawidłowości w ramach systemu, a jednocześnie będą zniechęcały do umyślnego dokonywania zgłoszeń fałszywych. Mamy nadzieję, że ustawodawca da możliwość elastycznego wdrożenia systemów zgłoszeniowych w podmiotach prywatnych, bez nadmiernych obwarowań formalnych.

OPIS ORGANIZACJI ORAZ FUNKCJONUJĄCEGO SYSTEMU WHISTLEBLOWINGOWEGO:

Grupa Tauron jest jednym z największych podmiotów gospodarczych w Polsce zatrudniającym ponad 25 tysięcy pracowników. Działa we wszystkich obszarach rynku energetycznego – od wydobycia węgla, poprzez wytwarzanie, dystrybucję i sprzedaż energii elektrycznej i ciepła oraz obsługę klienta.
W Grupie TAURON funkcjonuje System Zgłaszania Nadużyć stanowiący usystematyzowany ciąg następujących po sobie działań, służących przyjęciu i rozpatrzeniu otrzymanego zgłoszenia oraz poinformowania zgłaszającego o wynikach przeprowadzonego postępowania wyjaśniającego.
W ramach tego systemu umożliwia się sygnalizowanie działań niezgodnych z prawem oraz naruszeń regulacji wewnątrzkorporacyjnych za pośrednictwem przyjętych w Grupie TAURON kanałów komunikacji, tj.: -osobiście: do bezpośredniego przełożonego, Pełnomocnika ds. Compliance, Koordynatorów ds. Compliance w Spółkach Grupy TAURON, -pisemnie: na adres Pełnomocnika ds. Compliance lub na adres e-mail compliance@tauron.pl lub za pośrednictwem Formularza Zgłoszenia Nadużycia dostępnego na stronie https://www.tauron.pl/tauron/o-tauronie/formularz-zgloszenia-naduzycia Formularz Zgłoszenia Nadużycia dopuszcza możliwość przekazania informacji anonimowo. W przypadku ujawnienia tożsamości gwarantujemy poufność danych osoby zgłaszającej oraz przekazywanych informacji, -telefonicznie: dedykowany numer telefonu. Grupa TAURON zapewnia ochronę przed wszelkimi formami działań odwetowych osobom zgłaszającym w dobrej wierze przypadki nadużyć.

KORZYŚCI I WYZWANIA ZWIĄZANE Z FUNKCJONOWANIEM SYSTEMU ZGŁASZANIA NIEPRAWIDŁOWOŚCI:

KORZYŚCI:

- przekazane informacje o nieprawidłowych zachowaniach pozwalają na zidentyfikowanie nieprawidłowych zdarzeń oraz podjęcie niezbędnych działań naprawczych w celu wykluczenia możliwości zaistnienia podobnych zdarzeń w przyszłości,
- minimalizacja ryzyka strat finansowych i wizerunkowych,
- zwiększenie prawdopodobieństwa dokonania zgłoszenia wewnętrznego zanim sprawa zostanie zgłoszona poza organizację,
- zwiększenie prawdopodobieństwa wykazania dochowania należytej staranności przez organizację w przeciwdziałaniu nieprawidłowości
- budowanie pozytywnego wizerunku organizacji stosującej najlepsze praktyki rynkowe,
- rozwijanie kultury etycznej organizacji.

WYZWANIA:

- budowanie zaufania pracowników do systemu zgłaszania nieprawidłowości,
- budowanie pozytywnego wizerunku sygnalisty,
- rozpatrywanie lakonicznych zgłoszeń,
- prowadzenie postępowań wyjaśniających w ramach kilku spółek grupy kapitałowej,
- zapewnienie faktycznej ochrony przed działaniami odwetowymi osobie zgłaszającej nieprawidłowość (w ramach grupy kapitałowej) w szczególności w przypadku zgłoszeń anonimowych,
- zapewnienie zgodności funkcjonowania systemu whistleblowingowego z RODO (m.in. wypełnienie obowiązku informacyjnego, przetwarzanie danych szczególnych, retencja danych).

SZCZEGÓLNE OSIĄGNIĘCIA ZWIĄZANE Z SYSTEMEM ZGŁASZANIA NIEPRAWIDŁOWOŚCI:

1. Wdrożenie jednolitych rozwiązań w zakresie przyjmowania oraz rozpatrywania zgłoszeń w ramach całej Grupy kapitałowej,
2. Przeprowadzenie cyklu szkoleń dla Zarządów oraz kadry kierowniczej spółek (m.in. w siedzibach Spółek, on-line, w ramach Compliance Day),
3. Przeprowadzenie kampanii informacyjnej również także wśród pracowników nie mających dostępu do komputera,
4. Wprowadzenie zagadnień dot. compliance i zgłaszania nieprawidłowości do szkoleń onboardingowych pracowników,
5. Aktualizacja programów szkoleń okresowych BHP dla pracowników fizycznych zatrudnionych pod ziemią i na powierzchni, pracowników administracyjno – biurowych oraz osób kierujących pracownikami spółek górniczych o zagadnienia związane z compliance,
6. Otrzymanie nagrody Compliance Awards 2019 - Pomysł Compliance Roku za Kampanię antykorupcyjną Grupy TAURON.

OCZEKIWANIA WZGLĘDEM USTAWODAWCY W KONTEKŚCIE KSZTAŁTU USTAWY IMPLEMENTUJĄCEJ DYREKTYWĘ O SYGNALISTACH:

Ustawodawca implementując tzw. Dyrektywę o ochronie sygnalistów do krajowego porządku prawnego powinien uregulować następujące kwestie:

1. wprowadzenie do porządku prawnego definicji legalnej sygnalisty - osoby dokonującej zgłoszenia,

2. zdefiniowanie przesłanek warunkujących przyznanie/ odebranie statusu sygnalisty, w szczególności w przypadku gdy ujawnione informacje nie zostały potwierdzone w toku postępowania wyjaśniającego lub gdy osoba dokonująca zgłoszenia jest współsprawcą,

3. określenie zakresu przedmiotowego zgłoszeń objętych zakresem stosowania ustawy,

4. wprowadzenie katalogu środków ochronnych, które organizacji musi zapewnić sygnaliście,

5. wprowadzenie katalogu sankcji dla osób dokonujących zgłoszenia w złej wierze,

6. wprowadzenie katalogu obowiązków organizacji w stosunku do sygnalisty oraz sankcji za nie wypełnienie tych obowiązków o ile sygnalista działał w dobrej wierze,

6. uregulowanie kwestii odpowiedzialności sygnalisty w przypadku jednoczesnego naruszenia innych przepisów prawa (m.in. tajemnica przedsiębiorstwa, pomówienie, naruszenie dóbr osobistych),

7. zapewnienie spójności postanowień ustawy z postanowieniami kodeksu pracy, w szczególności w zakresie obowiązków pracowniczych (obowiązek informowania o nieprawidłowościach),

8. wprowadzenie hierarchii (kolejności) w zakresie kanałów zgłoszeń – wprowadzenie obowiązku korzystania w pierwszej kolejności z wewnętrznych kanałów zgłoszeń,

9. dopuszczenie możliwości wdrożenia jednego systemu whistleblowingowego obejmującego całą grupę kapitałową,

10. określenie zakresu wewnętrznej procedury w zakresie przyjmowania oraz rozpatrywania,

11. rozstrzygniecie obowiązku komunikowania się z osobą dokonującą anonimowego zgłoszenia (posiadania dedykowanej platformy/ narzędzia IT),

12. rozstrzygniecie obowiązku podejmowania działań w odniesieniu do zgłoszeń anonimowych, w szczególności w zakresie przekazywania informacji zwrotnej osobie dokonującej zgłoszenia,

13. wprowadzenie postanowień umożliwiających brak wszczęcia postępowania wyjaśniającego w sprawie będącej przedmiotem wcześniejszego zgłoszenia o ile nie zostały wskazane nowe okoliczności sprawy,

14. wprowadzenie postanowień będących podstawą prawną do przetwarzania danych osobowych, w tym danych szczególnej kategorii sygnalisty oraz osób, których dane pojawiają się w postępowaniu wyjaśniającym, w związku z funkcjonowaniem systemu whistleblowingowego – aktualnie istnieje możliwość przetwarzania danych osobowych jedynie na podstawie prawnie uzasadnionego interesu, co nie daje legitymacji do przetwarzania danych szczególnej kategorii.

15. doprecyzowanie okresu retencji przetwarzania danych osobowych w ramach systemu whistleblowingowego.

UDANE I PROBLEMATYCZNE KWESTIE ZWIĄZANE Z SYSTEMEM ZGŁASZANIA NIEPRAWIDŁOWOŚCI:

Co się udaje ?

1. Wzrost świadomości kadry zarządzającej nt. zagadnień związanych z compliance, w tym zgłaszaniem nieprawidłowości,

2. Ukierunkowanie działań na realizację funkcji prewencyjnej poprzez prowadzenie kampanii informacyjnych i szkoleń,

3. Wzmocnienie roli Compliance Officera w organizacji.

Problemy

1. Dotarcie z przekazem do wszystkich pracowników grupy kapitałowej, dostawców, podwykonawców itp.,

2. Prowadzenie postępowań wyjaśniających w przypadku lakonicznych, anonimowych zgłoszeń (np. w sprawach mobbingu),

3. Agregacja i spójne raportowanie danych do Zarządu i Rady Nadzorczej w ramach grupy kapitałowej.

NAJCIEKAWSZA HISTORIA ZWIĄZANA Z SYSTEMEM WHISTLEBLOWING:

Otrzymanie zgłoszenia wskazującego na nieprawidłowości w postępowaniu na dzierżawę gruntu. W toku postępowania wyjaśniającego ustalono, iż osoba wskazana jako nadawca zgłoszenia nie była jego rzeczywistym autorem, a był nim najprawdopodobniej inny, konkurencyjny podmiot, który zgłaszając nieprawidłowość dążył uzyskania korzystanego rozwiązania. Zgłoszenie zostało zakwalifikowane jako dokonane w złej wierze.

O ZESPOLE DZP COMPLIANCE

RAPORT ZOSTAŁ PRZYGOTOWANY PRZEZ SPECJALISTÓW Z ZESPOŁU COMPLIANCE KANCELARII DZP. POZNAJ NAS BLIŻEJ.

DZP to największa polska kancelaria prawnicza. Ponad 160 naszych ekspertów doradza polskim i zagranicznym klientom z niemal wszystkich branż gospodarki od ponad 25 lat.

9 praktyk i 40 specjalizacji | Biura w Warszawie, Poznaniu i Wrocławiu | Liczne rekomendacje i wysoka pozycja w międzynarodowych rankingach | 70 krajów w sieci relacji biznesowych.

CZYM ZAJMUJE SIĘ NASZ ZESPÓŁ?

▸ Analizą ryzyk w organizacji, którą stanowią m.in. mapowanie i ocena ryzyka, określanie procesów i procedur, jakie powinny funkcjonować w organizacji, identyfikacja słabych punktów systemu compliance.

▸ Wdrażaniem kompleksowych Compliance Management Systemes, polegających m.in. na tworzeniu regulacji wewnętrznych, przypisywaniu zadań poszczególnym członkom organizacji, budowie mechanizmów przeciwdziałania nadużyciom oraz systemów whistleblowingowych.

▸ Wykrywaniem i reagowaniem, w ramach czego przeprowadzamy audyty i postępowania wyjaśniające związane z wykrytą lub możliwą nieprawidłowością.

▸ Edukacją i prewencją, które obejmują głównie doradztwo compliance „day-by-day", szkolenia pracownicze i warsztaty dla managementu prowadzone prostym językiem i oparte na praktycznych przykładach.

▸ Komunikacją wewnętrzną w organizacji, tj. upraszczaniem języka instrukcji i procedur wewnętrznych, analizą komunikacji pracowniczej (audyty e-mail), prowadzeniem warsztatów o roli prawidłowej komunikacji w zapewnianiu bezpieczeństwa organizacji i pracowników.

W CZYM JUŻ POMOGLIŚMY?

Projekty compliance i doradztwo bieżące

▸ Budowa i wdrożenie złożonych systemów zarządzania zgodnością i systemów antykorupcyjnych w wielu spółkach z międzynarodowych grup kapitałowych w oparciu o normy ISO 19600 Compliance Management System, 37001 Anti-bribery Management System i 37002 Whistleblowing Management System.

▸ Analiza i udoskonalanie systemów compliance w firmach operujących w różnych sektorach i krajach w oparciu o FCPA, UKBA, Sapin II oraz wytyczne GPW.

▸ Kompleksowe przeszkolenie pracowników i kadry zarządzającej.

▸ Wdrożenie i outsourcing systemów whistleblowing, kampanie edukacyjne dla pracowników.

▸ Doradztwo bieżące „compliance day-to-day" i projekty doraźne w ramach zarządzania kryzysowego.

▸ Postępowania wyjaśniające z udziałem sygnalistów czy dedykowane investigations m.in. w przypadku podejrzenia korupcji gospodarczej i urzędniczej, nadużyć pracowników oraz naruszenia zasad uczciwej konkurencji.

▸ Mapowanie i ocena ryzyka w największych polskich spółkach i wdrażanie narzędzi zarządzania zidentyfikowanymi ryzykami.

▸ Wsparcie w procesie weryfikacji kontrahentów, komunikacji pracowniczej, audyty śledcze, monitoring legislacyjny.

GŁÓWNE OBSZARY DORADZTWA

ANALIZA I BIEŻĄCE DORADZTWO COMPLIANCE	AUDYTY I POSTĘPOWANIA WYJAŚNIAJĄCE (FORENSIC)	DUE DILIGENCE
SYSTEMY WHISTLEBLOWING	IMPLEMENTACJA ANTYKORUPCYJNEJ NORMY ISO 37001:2016	ZARZĄDZANIE KRYZYSOWE

AUTORZY RAPORTU

Julia Besz, LL.M
Associate / Zespół Compliance

Jakub Dydak
Associate / Zespół Compliance

Jan Bednarski
Associate / Zespół Compliance

Klaudia Sałdan
Associate / Zespół Compliance

Aleksandra Zomerska
Associate / Zespół Ochrony
Danych Osobowych

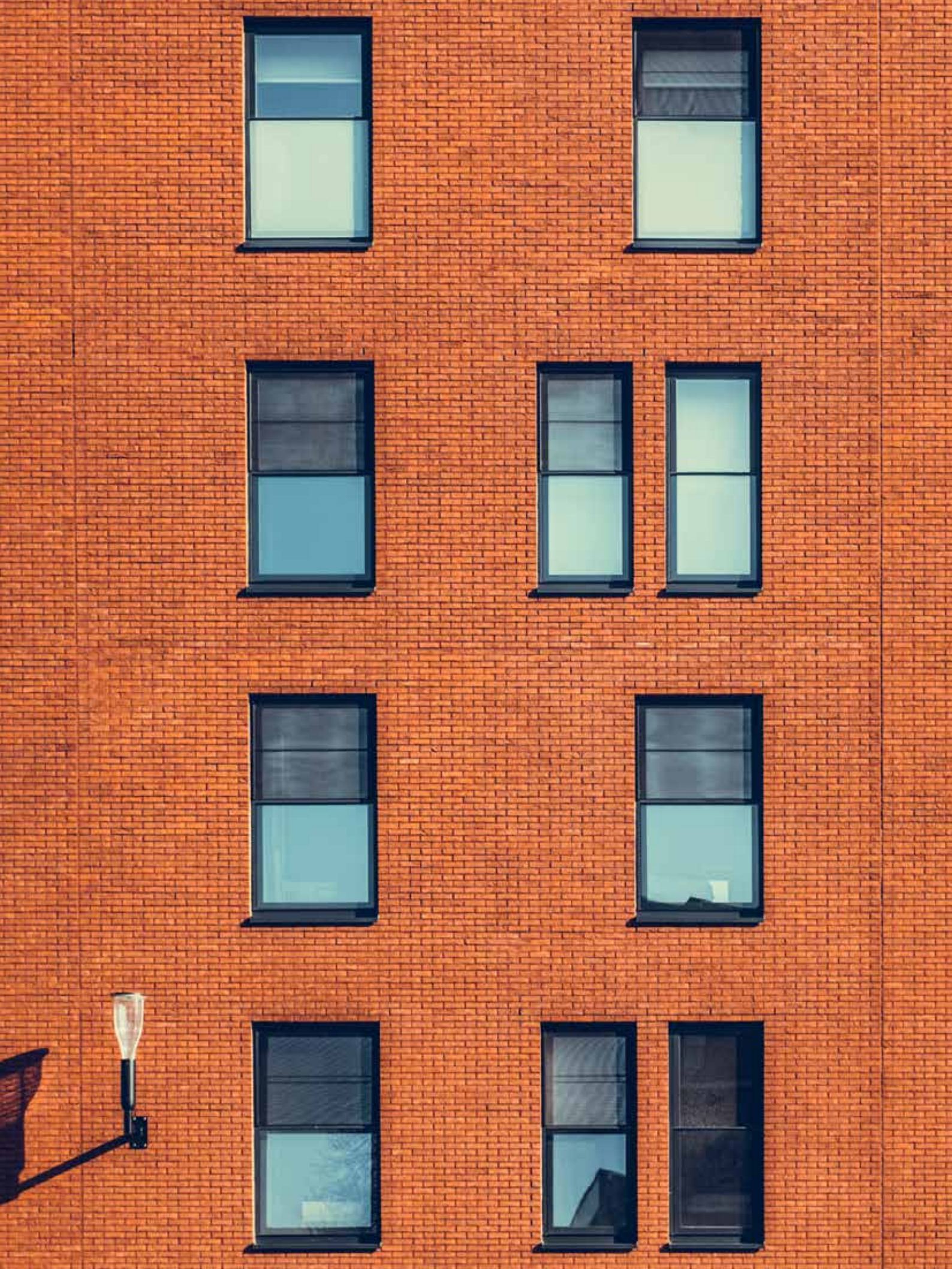
Barbara Lorenz
Associate / Zespół Compliance

REDAKCJA

Julia Besz, LL.M
Associate / Zespół Compliance

NADZÓR MERYTORYCZNY

dr Anna Partyka-Opiela
Partner / Zespół Compliance



PRZY WSPARCIU:

Global Compact
Network Poland

UNITED NATIONS GLOBAL COMPACT

Największa na świecie inicjatywa skupiająca biznes działający na rzecz zrównoważonego rozwoju. Zainaugurowana przez Sekretarza Generalnego ONZ w 2000 r. Skupia firmy tworzące strategie i działania w oparciu o dziesięć uniwersalnych zasad (10 Principles) w obszarach praw człowieka, standardów pracy, ochrony środowiska, przeciwdziałania korupcji oraz podejmowania działań pomagających osiągnąć Cele Zrównoważonego Rozwoju ONZ (SDGs).

UN GLOBAL COMPACT NETWORK POLAND

Sieć krajowa z niezależnym sekretariatem prowadzonym oraz zarządzanym przez Fundację Global Compact Poland. Stanowi biuro projektowe oraz lokalny punkt kontaktowy i informacyjny dla polskich członków oraz sygnatariuszy UN Global Compact. Identyfikuje wyzwania i możliwości w zakresie zrównoważonego rozwoju. Zapewnia praktyczne wskazówki oraz promuje działania na rzecz realizacji celów ONZ. Dodatkowo UN GCNP wspiera merytorycznie polskich członków UN Global Compact w wypełnianiu rocznego obowiązku raportowania niefinansowego, z podejmowanych przez firmę działań i osiągniętych rezultatów.

PROGRAM STANDARD ETYKI W POLSCE

Program realizowany przez UN GCNP w partnerstwie z biznesem ma na celu implementację wytycznych ONZ ds. biznesu i praw człowieka w Polsce oraz ich praktyczne zastosowanie w programach etycznych, w firmach i instytucjach. Program wspiera aktywność biznesu w obszarze promocji równości płci, różnorodności, ochrony sygnalistów, wdrażania standardówetycznych, rozwoju filantropii korporacyjnej.

AUTOR RAPORTU I OPRACOWANIA MERYTORYCZNEGO:

DZP
więcej niż prawo

Domański Zakrzewski
Palinka sp. k.
Rondo ONZ 1
00-124 Warszawa

PRZY WSPARCIU:

UN Global Compact
Network Poland

UN Global Compact
Network Poland
ul. Emilii Plater 25/64
00-688 Warszawa

REDAKCJA:
Julia Besz, LL.M | DZP

KOORDYNACJA PROJEKTU:
Jakub Dydak | DZP
Beata Chojecka | UNGC NP
Anna Potocka-Domin - UNGC NP

NADZÓR MERYTORYCZNY:
Anna Partyka-Opiela | DZP

PROJEKT GRAFICZNY I SKŁAD:
Agnieszka Skopińska
www.rebelzoo.eu

ZDJĘCIA:
unsplash.com

Network Poland

DZP
więcej niż prawo

Rondo ONZ 1
00-124 Warszawa
www.dzp.pl

PRZY WSPARCIU:

Global Compact
Network Poland

ul. Emilii Plater 25/64
00-688 Warszawa
www.ungc.org.pl