WHISTLEBLOWING
– wymóg prawny i wyzwanie dla sektora bankowego w Polsce

Do tej pory **w Polsce nie uregulowano w sposób kompleksowy zagadnienia ochrony sygnalistów** (ang. whistleblowers), czyli osób, które działając w dobrej wierze, informują o nieprawidłowościach lub zachowaniach nieetycznych godzących w interes pracodawcy i/lub dobro publiczne. W naszym kraju **jedynie sektor bankowy posiada w tym obszarze prawne regulacje** i to od niedawna, w związku z czym jeszcze nie zdążyła wytworzyć się odpowiednia praktyka w dziedzinie ochrony sygnalistów. Czas pokaże, czy banki sprostają temu wyzwaniu i staną się wzorcem dla innych dziedzin życia gospodarczego kraju.

Rafał Hryniewicz, prezes zarządu E-nform, analityk kryminalny i kontroler wewnętrzny, specjalista w zakresie analizy strategicznej, wywiadowczej i kryminalnej

Ustawą z dnia 5 sierpnia 2015 r. o nadzorze makroostrożnościowym nad systemem finansowym i zarządzaniu kryzysowym w systemie finansowym (dalej: ustawa o nadzorze) wprowadzono do art. 9 ustawy z dnia 29 sierpnia 1997 r. Prawo bankowe przepisy dotyczące anonimowego zgłaszania nadużyć w banku[1], tj.:

- ust. 2a. **System zarządzania obejmuje procedury anonimowego zgłaszania** wskazanemu członkowi zarządu, a w szczególnych przypadkach – radzie nadzorczej banku, **naruszeń prawa oraz obowiązujących w banku procedur i standardów etycznych**.
- ust. 2b. W ramach procedur, o których mowa w ust. 2a, **bank zapewnia pracownikom, którzy zgłaszają naruszenia, ochronę** co najmniej przed działaniami o charakterze represyjnym, dyskryminacją lub innymi rodzajami niesprawiedliwego traktowania.

Ponadto ustawa o nadzorze wprowadziła do Prawa bankowego art. 9f ust. 1 zobowiązujący Ministra właściwego do spraw instytucji finansowych do określenia w trybie rozporządzenia m.in. trybu anonimowego zgłaszania wskazanemu członkowi zarządu lub rady nadzorczej naruszeń prawa oraz obowiązujących w banku procedur i standardów etycznych. Był to pierwszy przepis w obszarze prawa w Polsce otwierający drogę do prawnego uregulowania kwestii **ochrony sygnalistów**. Należy jednak dodać, że nie była to inicjatywna polskiego ustawodawcy, ale implementacja art. 71 tzw. dyrektywy CRD IV[2], która nałożyła na Państwa członkowskie UE **obowiązek ustanowienia skutecznych i niezawodnych mechanizmów sygnalizowania właściwym organom potencjalnych lub faktycznych naruszeń przepisów** krajowych w obszarze regulowanym niniejszą dyrektywą oraz rozporządzeniem Parlamentu Europejskiego i Rady (UE) nr 575/2013"[3].

Wykonaniem delegacji ustawowych zawartych we wspomnianym wyżej art. 9f ust. 1 pkt 2 Prawa bankowego było wprowadzenie z dniem 1 maja 2017 roku do polskiego porządku prawnego Rozporządzenia Ministra Rozwoju i Finansów z dnia 6 marca 2017 r. (dalej: Rozporządzenie) w sprawie systemu zarządzania ryzykiem i systemu kontroli wewnętrznej, polityki wynagrodzeń oraz szczegółowego sposobu szacowania kapitału wewnętrznego w bankach. Jest

1. Przepisy te weszły w życie z dniem 1 listopada 2015 roku.

2. Dyrektywa Parlamentu Europejskiego i Rady 2013/36/UE z dnia 26 czerwca 2013 r. w sprawie warunków dopuszczenia instytucji kredytowych do działalności oraz nadzoru ostrożnościowego nad instytucjami kredytowymi i firmami inwestycyjnymi, zmieniająca dyrektywę 2002/87/WE i uchylająca dyrektywy 2006/48/WE oraz 2006/49/WE (Capital Requirements Directive IV, **CRD IV**).

3. Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 575/2013 z dnia 26 czerwca 2013 r. w sprawie wymogów ostrożnościowych dla instytucji kredytowych i firm inwestycyjnych, zmieniające rozporządzenie (UE) nr 648/2012.

to pierwszy tego typu akt prawny, który szczegółowo reguluje zagadnienie whistleblowingu w obszarze regulowanym Prawem bankowym. Procedurom anonimowego zgłaszania naruszeń prawa oraz obowiązujących w banku procedur i standardów etycznych poświęcony jest rozdział 5 (§ 45) Rozporządzenia. Wskazuje on m.in., że **pracownicy banku powinni mieć możliwość zgłaszania naruszeń za pośrednictwem specjalnego, niezależnego i autonomicznego kanału komunikacji**, a procedury związane z sygnalizowaniem nieprawidłowości powinny określać co najmniej:

- **sposób odbierania zgłoszeń** w sprawie naruszeń, zapewniając anonimowość pracownikom przekazującym informacje,
- **sposób ochrony pracowników** dokonujących zgłoszeń, co najmniej przed działaniami o charakterze represyjnym, dyskryminacją lub innym niesprawiedliwym oddziaływaniem,
- **sposób ochrony danych osobowych** nie tylko pracownika dokonującego zgłoszenia, ale także osoby, której zarzuca się dokonanie naruszenia – w przypadku negatywnej weryfikacji zasadności zgłoszenia naruszenia, bank obowiązany jest niezwłocznie usunąć ze swoich systemów dane osobowe zawarte w tym zgłoszeniu,
- sposób ochrony pracownika zgłaszającego nieprawidłowości, w przypadku jeżeli ujawnił swoją tożsamość, lub jest ona możliwa do ustalenia,
- **wskazanie osób odpowiedzialnych za odbieranie zgłoszeń naruszeń,**
- **sposób postępowania ze zgłoszeniem**, w tym przekazywania go wskazanemu członkowi zarządu lub radzie nadzorczej,
- **termin usunięcia przez bank danych osobowych** zawartych w zgłoszeniach naruszeń,
- **termin powiadomienia podejrzewanej o naruszenie osoby o dokonanym zgłoszeniu** oraz o przeprowadzonej procedurze weryfikacji, w przypadku pozytywnej weryfikacji zgłoszenia o naruszeniu.

Ponadto, zgodnie z Rozporządzeniem **zarząd ponosi odpowiedzialność za adekwatność i skuteczność procedur anonimowego zgłaszania naruszeń**, natomiast **rada nadzorcza dokonuje ich oceny**. Rozporządzenie nakłada również obowiązek przeprowadzania regularnych szkoleń dla pracowników z obowiązujących procedur dotyczących zgłaszania naruszeń.

Wprowadzone w życie przepisy Rozporządzenia stworzyły dla „bankowego whistleblowingu" dogodne otoczenie prawne i należy mieć nadzieję, że zostanie to efektywnie wykorzystane przez polski sektor bankowy. Nie jest tajemnicą, że whistleblowing to najskuteczniejsze narzędzie do wykrywania nieprawidłowości. Według Stowarzyszenia Certyfikowanych Ekspertów ds. Oszustw (ACFE – Association of Certified Fraud Examiners) w odniesieniu do nadużyć pracowniczych (np. kradzieży, łapówek, fałszerstw), **systemy wewnętrznego, anonimowego sygnalizowania nieprawidłowości wykazują największą skuteczność** (około 40% przypadków) spośród wszystkich narzędzi wykrywania tego typu zjawisk[4]. Kolejne z najskuteczniejszych narzędzi, czyli audyt wewnętrzny jest znacznie mniej efektywne (ok. 15% przypadków). Natomiast doświadczenia firmy doradczej PwC Polska pokazują, że na 338 projektów śledczych, 69% z nich zostało zainicjowanych dzięki informacjom sygnalistów, 22% przez informacje kontroli wewnętrznej i 9% przez informacje z innych źródeł[5]. Symptomatyczne dla polskiego, bardzo powoli rozwijającego się whisttleblowingu jest to, że **73% sygnalistów pozostało anonimowych**, co nie może dziwić, mając na uwadze fakt, że 58% osób przewiduje negatywną reakcję ze strony zespołu wobec sygnalisty (okazywanie dystansu, złośliwe komentarze, wykluczenie z zespołu koleżeńskiego, jawne ignorowanie). Dlatego też od skuteczności wdrożenia systemu zgłaszania nieprawidłowości w organizacji, uwzględniającej bezpieczeństwo sygnalistów, zależy jego efektywność.

Jak więc skutecznie wdrożyć taki system w organizacji, w tym banku? Z pewnością jest to proces złożony i długotrwały, wymagający wielopłaszczyznowego, konsekwentnego i odpowiedzialnego działania. Wdrażając taki system trzeba pamiętać w szczególności o następujących elementach:

- pełne wsparcie kierownictwa organizacji dla systemu zgłaszania naruszeń,
- określenie i kształtowanie kultury etycznej organizacji (kodeksy etyczne, polityki antykorupcyjne, etc.),
- zdefiniowanie nieprawidłowości/zachowań niepożądanych oraz zagrożeń adekwatnych do organizacji (m.in. analiza ryzyka, badania ankietowe, etc.),
- integracja pracowników z organizacją (zaangażowanie w budowę systemu, procedur, identyfikację zagrożeń, etc.),
- objęcie systemem wszystkich pracowników oraz obszarów funkcjonowania organizacji,
- powierzenie funkcji zarządzania zgłoszeniami osobom kompetentnym, niezależnym, bezstronnym i cieszącym się zaufaniem pracowników,
- wdrożenie efektywnego nadzoru nad funkcjonowaniem systemu (zarząd, rada nadzorcza),
- wdrożenie procedur dot. zgłaszania nieprawidłowości oraz zasad ochrony sygnalistów zgodnie z wymogami *Rozporządzenia* (deklaracje poparte faktycznymi działaniami),
- wdrożenie mechanizmów umożliwiających skuteczne i bezpieczne przekazywanie informacji o nieprawidłowościach (skrzynki mailowe, programy komputerowe, telefony),
- prowadzenie wstępnych, a następnie regularnych szkoleń dla pracowników z zakresu whistleblowingu, a także kultury etycznej organizacji,
- rzetelne zarządzanie zgłoszeniami.

Wdrażany system zgłaszania naruszeń powinien być spójny z systemem zarządzania w organizacji i opierać się na zaufaniu między pracownikami i kierownictwem. Oczywiście każda zmiana w organizacji, związana m.in. z wdrożeniem takiego systemu zawsze budzi dyskomfort, a nierzadko i niechęć do niej części pracowników, w tym kadry zarządzającej, ale efektywne zaangażowanie ich w jego budowę może przynieść bardzo pozytywne efekty. Należy również pamiętać, aby walczyć ze stereotypami związanymi ze zgłaszaniem nieprawidłowości, w szczególności w trybie anonimowym. Nierzadko zgłaszanie nadużyć ma pejoratywne

4. Report to the Nations on Occupational Fraud and Abuse 2012 Global Fraud Study, ACFE 2012.

5. Sygnalista po Polsku – dobre praktyki i rekomendacje wdrożeniowe, PwC 2017.

>>

zabarwienie, gdyż kojarzone jest z donoszeniem, które swoje piętno wywarło na naszym społeczeństwie funkcjonującym w systemie politycznym sprzed 1990 roku.

Jednym z najistotniejszych aspektów wdrażania systemu zgłaszania nadużyć jest wybór odpowiedniego narzędzia do komunikacji z sygnalistami. Najczęściej są to skrzynki mailowe utworzone w ramach organizacji i zarządzane przez komórkę compliance. Dobrą stroną takiego rozwiązania może być to, że informacje o nieprawidłowościach pozostają w organizacji, a ich właściwa interpretacja przez wyznaczonego pracownika tej organizacji nie powinna rodzić problemów. Wadami takiego rozwiązania może być m.in. możliwość ustalenia przez administratora systemu informatycznego nie tylko adresu mailowego ale także IP komputerów służbowych pracowników, z których dokonywane są zgłoszenia. Ponadto skrzynka mailowa nie posiada funkcjonalności umożliwiających skuteczne zarządzanie pozyskaną informacją, w tym nierzadko prowadzenia efektywnego i bezpiecznego dialogu z sygnalistą. Problem rodzi się również wtedy, gdy za zarządzenie zgłoszeniami odpowiedzialna jest komórka organizacyjna, lub osoba nie ciesząca się zaufaniem pracowników. W takiej sytuacji niejednokrotnie zdarza się, że do systemu zgłoszeniowego organizacji zatrudniającej tysiące pracowników nie trafiają żadne zgłoszenia, a o nieprawidłowościach, które w tej organizacji mają miejsce, można przeczytać w mediach.

Drugie rozwiązanie polega na powierzeniu przez organizację (zleceniodawca) zarządzania zgłoszeniami podmiotowi zewnętrznemu (zleceniobiorca), który posiada swoje kanały komunikacyjne (skrzynki mailowe, numery telefoniczne). W tym przypadku bezpieczeństwo sygnalistów jest na znacznie wyższym poziomie i nie powinno być również obaw o bezstronność obsługi zgłoszeń.

Wadami tego rozwiązania mogą być natomiast dość wysokie, stałe koszty obsługi zgłoszeń, a przede wszystkim brak dostępu do informacji, które trafiają do takiego zewnętrznego podmiotu. Należy pamiętać, że informacje przekazywane przez sygnalistów to nierzadko informacje prawnie chronione, w postaci tajemnicy przedsiębiorstwa, czy też danych osobowych, a także inne informacje wrażliwe o organizacji (nieprawidłowości, nadużycia, etc.), których utrata może przynieść poważne skutki zarówno dla wizerunku zleceniodawcy jak i jego finansów. Niestety zleceniodawca nie ma bezpośredniego wpływu na sposób zrządzania tymi informacjami i musi w tym zakresie ufać zleceniobiorcy, zabezpieczając się stosownymi umowami o poufności. Ponadto może się zdarzyć, że obsługujący zgłoszenia zleceniobiorca może źle zinterpretować informacje przekazywane przez sygnalistów, z uwagi na nieznajomość branży lub specyfiki organizacji. Podobnie, jak w pierwszym rozwiązaniu, także i w tym funkcjonalności związane z zarządzaniem informacji są dość ubogie.

Należy podkreślać, że whistleblowing to przejaw odwagi i odpowiedzialności za organizację, a przymykanie oczu na nadużycia to de facto cichy w nich współudział i nierzadko okradanie samego siebie.

Trzecie rozwiązanie polega na zakupie licencji terminowej lub bezterminowej na użytkowanie dedykowanego oprogramowania komputerowego posiadającego własną szyfrowaną bazę danych, w którym gromadzone są zgłoszenia. W takiej sytuacji zleceniodawca jest właścicielem wrażliwych danych dotyczących jego organizacji, a ponadto uzyskuje bezpieczne narzędzie komunikacyjne o rozbudowanych możliwościach, które nierzadko mogą być dostosowane do specyfiki jego organizacji. Takie rozwiązanie nie musi być wcale droższe od drugiego rozwiązania, a daje znacznie większe bezpieczeństwo informacji i rozbudowane funkcjonalności zarządzania informacją. Wadą może być natomiast powierzenie zarządzania takim oprogramowaniem niewłaściwym osobom (brak zaufania ze strony pracowników, niekompetencja). W takim przypadku zalecane jest powierzenie obsługi oprogramowania profesjonalnemu i godnemu zaufania podmiotowi, przy jednoczesnym nadzorze nad gromadzonymi w aplikacji informacjami.

Oczywiście każda organizacja może sama zbudować odpowiednie narzędzie informatyczne lub zlecić jego wykonanie podmiotowi zewnętrznemu, ale trzeba pamiętać, że wiąże się to z koniecznością zapewnienia kompetentnej kadry i stosownego budżetu, uwzględniającego również wszelkie zmiany w oprogramowaniu.

Przy wyborze odpowiedniego rozwiązania należy zawsze pamiętać w szczególności o:

- bezpieczeństwie osób zgłaszających nieprawidłowości,
- bezpieczeństwie informacji trafiających do systemu (szyfrowanie, dostępność dla organizacji),
- właściwym przetwarzaniu danych osobowych w systemie (m.in. możliwość ich usuwania),
- możliwościach efektywnego zarządzania informacją (historia zgłoszenia i sposób jego obsługi, statystyka, etc.),
- możliwościach dostosowywania rozwiązania m.in. do zmieniających się wymogów prawnych,
- zapewnieniu kompetentnych, rzetelnych i bezstronnych osób do obsługi zgłoszeń,
- długofalowych kosztach wdrożenia danego rozwiązania.

Podsumowując niniejsze zagadnienie warto również zastanowić się nad tym, czy wdrożonego bezpiecznego i efektywnego kanału komunikacyjnego między pracownikami i najwyższym kierownictwem nie wykorzystać także do pozyskiwania informacji o wszelkich pomysłach umożliwiających zwiększenie przewagi konkurencyjnej organizacji na rynku (redukcja kosztów, zwiększenie zysków, usprawnienie pracy). Ponadto każda organizacja powinna również rozważyć możliwość otwarcia się na informacje od swoich kontrahentów, czy też klientów, co mogłoby przynieść zupełnie nowe spojrzenie nie wiele kwestii związanych z jej funkcjonowaniem. ●