KNF | KOMISJA NADZORU FINANSOWEGO

Łukasz Cichy

Whistleblowing w bankach

Łukasz Cichy

WHISTLEBLOWING W BANKACH

Warszawa 2017

KNF | KOMISJA NADZORU FINANSOWEGO

Publikacja została wydana nakładem Komisji Nadzoru Finansowego

Pl. Powstańców Warszawy 1
00-030 Warszawa
www.knf.gov.pl

Warszawa 2017
Wydanie I

ISBN 978-83-63380-17-5

Nakład: 1500 szt.

Stan prawny na dzień: 1 czerwca 2017 r.

Przygotowanie do druku i druk:
EXPOL P. Rybiński, J. Dąbek, sp.j.

SPIS TREŚCI

I. WSTĘP

Gdy w 1971 r. konsumencki aktywista Ralph Nader apelował dosłownie o gwizdanie (*blow the whistle*) w odniesieniu do korporacyjnych skandali, pewnie nie zdawał sobie sprawy, jak długą drogę przejdzie idea whistleblowingu do czasów obecnych. Dziś informowanie o nadużyciach uważane jest za powszechne narzędzie wspomagające skuteczne zarządzanie, niemniej jednak wciąż budzi ono poważne wątpliwości interpretacyjne. Niniejsze opracowanie ma przybliżyć ideę whistleblowingu przede wszystkim w kontekście zarządzania bankiem, jak i umieścić ją, na tyle, na ile to możliwe, w kontekście podstawowych obowiązków prawnych. Dokument adresowany jest przede wszystkim do pracowników banków, zwłaszcza tych pełniących kierownicze funkcje, a także osób zainteresowanych zagadnieniem whistleblowingu w bankowości.

II. SŁOWNIK POJĘĆ

Dyrektywa CRD IV – 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).

Rozporządzenie MRiF – Rozporządzenie Ministra Rozwoju i Finansów z dnia 6 marca 2017 r. w sprawie systemu zarządzania ryzykiem i systemu kontroli wewnętrznej, polityki wynagrodzeń oraz szczegółowego sposobu szacowania kapitału wewnętrznego w bankach (Dz.U. poz. 637).

Rozporządzenia MAR – Rozporządzenie Parlamentu Europejskiego i Rady (UE) Nr 596/2014 z dnia 16 kwietnia 2014 r. w sprawie nadużyć na rynku (rozporządzenie w sprawie nadużyć na rynku) oraz uchylające dyrektywę 2003/6/WE Parlamentu Europejskiego i Rady i dyrektywy Komisji 2003/124/WE, 2003/125/WE i 2004/72/WE (Dz.U. UE L 173/1 z dnia 12.6.2014).

Ustawa – ustawa z dnia 29 sierpnia 1997 r. – Prawo bankowe (Dz.U. z 2016 r. poz. 1988, z późn. zm.).

Whistleblowing – raportowanie przez obecnych lub byłych pracowników o nielegalnych, niewłaściwych, niebezpiecznych lub nieetycznych praktykach pracodawców.

Whistleblower/sygnalista – osoba dokonująca zgłoszenia naruszeń w ramach whistleblowingu.

III. DEFINICJA I RATIO LEGIS

Samo pojęcie whistleblowingu wciąż nie doczekało się jednoznacznej, powszechnie uznawanej definicji, co nastręczać może problemów zarówno ustawodawcom i regulatorom, jak i samym organizacjom, w tym bankom. Najczęściej używaną definicją jest definicja autorstwa Jabet Near i Marici Miceli z 1985 r., wedle której whistleblowing to „ujawnienie przez obecnych lub byłych członków organizacji nielegalnych, niemoralnych lub niedopuszczalnych praktyk prowadzonych pod nadzorem/kontrolą ich pracodawców, osobom lub organizacjom, które są w stanie przedsięwziąć działania”[1]. Bardziej szczegółową i dość popularną definicję zaprezentował Peter Jubb[2], dodatkowo podkreślający wymóg dobrowolności zgłoszenia, dostępu do informacji, wagi naruszenia (nie powinno być trywialne) oraz – co może budzić zdziwienie – ujawniania podmiotom zewnętrznym. Z kolei wielce ogólną, a przez co jednocześnie elastyczną definicję zaprezentowała Międzynarodowa Organizacja Pracy, wedle której whistleblowing to po prostu „raportowanie przez obecnych lub byłych pracowników o nielegalnych, niewłaściwych, niebezpiecznych lub nieetycznych praktykach pracodawców[3]. W tym rozumieniu whistleblowing będzie używany w niniejszej publikacji.

---

[1] J. P. Near, M. P. Miceli, *Organizational Dissidence: The Case of Whistleblowing*, “Journal of Business Ethics” 4/1985, s. 4.

[2] P. B. Jubb, *Whistleblowing: A Restrictive Definition and Interpretation*, “Journal of Business Ethics” 21/1999, s. 83 za H. Hasink, M. de Vries, L. Bollen, *A Content Analysis of Whistleblowing Policies of Leading European Companies*, “Journal of Business Ethics”, 75/2007, s. 25.

[3] International Labour Organization, *Thesaurus*, 2005, za D. Banisar, *Whistleblowing: International Standards and Developments*, [w:] *Corruption and transparency: debating the frontiers*

Oprócz kolejnych prób definicji, czym whistleblowing jest, warto podkreślić także, czym whistleblowing nie jest. Za Davidem Banisarem[4] można powtórzyć, iż whistleblowing nie jest informowaniem o nadużyciach przez współsprawców w zamian za złagodzenie kary. Nie jest także informowaniem w ramach tzw. programu ochrony świadków. Z whistleblowingiem nie mamy też do czynienia w przypadku, gdy na danej osobie ciąży obowiązek informacji (np. audytor wewnętrzny składający raport).

Zestawiając powyższe definicje, można więc wyróżnić podstawowe rodzaje whistleblowingu – to jest whistleblowing wewnętrzny (w ramach danej organizacji – np. banku) oraz whistleblowing zewnętrzny (do podmiotu zewnętrznego – np. regulatora). Oba rodzaje zostały wprowadzone w nowelizacji ustawy – Prawo bankowe (zwanej dalej „ustawą"), odpowiednio w art. 9 ust. 2a-2b, art. 133a ust. 9 i 10 ustawy, ale tylko ten pierwszy, czyli whistleblowing wewnętrzny, będzie przedmiotem niniejszego opracowania.

RATIO LEGIS

Szczegółowe badania wskazują, że powodów, dla których ustawodawca, regulator czy dana organizacja decydują się na wprowadzenie whistleblowingu, jest wiele. Zdaniem wieloletniego badacza, Wima Vandekerckhove'a[5], whistleblowing wprowadzany jest z racji ośmiu podstawowych powodów, tj. perspektywy:

- praw człowieka – zgłaszanie naruszeń jako element praw człowieka, w tym zwłaszcza prawa do wolności słowa każdego z pracowników,
- sieci powiązań – whistleblowing umożliwia równowagę sił pomiędzy uczestnikami sieci społecznych, pozwalającą redukować przewagę i wzmacniać zaufanie,
- interesariuszy – whistleblowing jako sygnał ostrzegawczy dla interesariuszy, że dana organizacja przestaje realizować szeroko rozumiane cele dobra społecznego,

between state, market and society, I. Sandoval, ed., World Bank-Institute for Social Research, UNAM, Washington, 1.02.2011, s. 6.

[4] D. Banisar, Ibidem, s. 6–8.

[5] W. Vandekerckhove, *Whistleblowing and Organizational Social Responsibility: A Global Assessment*, Ashgate 2006, s. 73–142.

- odpowiedzialności za wykonanie danego zadania – whistleblowing redukuje przesadny wzrost autonomii menadżerów, którzy otrzymują ją w ramach podziału zadań w procesie podejmowania decyzji,
- odpowiedzialności za rezultat danego zadania – whistleblowing jako „straszak" dla menadżerów niższego szczebla, którzy odpowiadają za osiąganie danych rezultatów,
- lojalności – whistleblowing jako element lojalności dla wartości, którymi kieruje się dana organizacja, wyrażanych np. w kodeksach etycznych,
- integralności – whistleblowing jako element etycznej integralności organizacji i jej pracowników,
- skuteczności – whistleblowing zewnętrzny jako skuteczny mechanizm transparentności organizacji, whistleblowing wewnętrzny jako swoisty strażnik (*watchdog*).

Wiele z powyższych racjonalizacji daje się wpisać w szeroko rozumiane zarządzanie ryzykiem. Tak postrzegany whistleblowing nie jest więc niczym innym jak prewencyjnym, ale także i korekcyjnym mechanizmem kontroli ryzyka, i to nie tylko np. ryzyka defraudacji czy wręcz ryzyka katastroficznego, ale także ryzyka nadużywania władzy w danej organizacji, czy też ryzyka reputacji[6].

Mimo powyższego, rozbudowanego ratio legis, niemal od początku swojego istnienia zgłaszanie naruszeń w ramach whistleblowingu napotykało na dylematy moralne, a przez wielu postrzegane było (i wciąż jest) bądź jako szpiegostwo wewnętrzne[7], bądź wręcz jako donosicielstwo. Przez wiele lat fundamentalne pytanie, przed jakim stawali nie tylko potencjalni zgłaszający, ale również i ci, którzy uprawnienie do wewnętrznego i zewnętrznego whistleblowingu ustanawiali, brzmiało: czy whistleblowing jest moralnie dopuszczalny, a jeśli tak, to czy i pod jakimi warunkami[8]. Zgodnie jednak z tzw.

---

[6] R. Ionescu, *Whistleblowing and disaster risk reduction*, [w:] *Developments in Whistleblowing Research 2015*, pod red. D. Levis, W. Vandekerckhove, Whistleblowing Research International Network 2015, s. 54.

[7] Tak na przykład w 1971 r. nazwał je J. Roche, przewodniczący rady dyrektorów General Motors, za W. Vandekerckhove, *Whistleblowing and Organizational*…, op. cit. s. 7–8.

[8] Szerzej patrz np. R.T. De George, *Whistle-blowing*, Business Ethics 1986, NY Macmillan Publishing Company za W. M. Hoffman, R. E. McNulty, *A business ethics theory of whistleblowing: responding to the $1 trillion question*, [w:] *Whistleblowing: In defense of proper action*, *Praxiology: The International Annual of Practical Philosophy and Methodology*, pod red. M. Arszułowicza, W. W. Gasparskiego. Transaction Publishers, 2011, s. 47.

nowym modelem whistleblowingu, współcześni ustawodawcy, co do zasady, nie uzależniają dopuszczalności zgłoszenia od motywacji zgłaszającego, kluczowa jest bowiem sama informacja, jej jakość i prawdziwość, bez względu na powody, jakimi kierował się sygnalista.

IV. WHISTLEBLOWING WEDŁUG PRZEPISÓW MIĘDZYNARODOWYCH I PRZEPISÓW KRAJOWYCH WYBRANYCH PAŃSTW

PRAWO MIĘDZYNARODOWE EUROPEJSKIE

Na poziomie europejskim brak jest kompleksowych rozwiązań dotyczących whistleblowingu oraz ochrony sygnalistów, obejmujących wszystkie sektory, a nie tylko np. sektor finansowy. Niemniej do najczęściej przywoływanych aktów prawnych w Europie należą:

- Konwencja o ochronie praw człowieka i podstawowych wolności – art. 10 dotyczący wolności wyrażania opinii wraz z orzecznictwem,
- Karta praw podstawowych Unii Europejskiej – art. 11 dotyczący wolności wypowiedzi i informacji, art. 30 dotyczący ochrony w przypadku nieuzasadnionego zwolnienia z pracy, art. 47 prawo do skutecznego środka prawnego i dostępu do bezstronnego sądu,
- Rezolucja nr 2060 Rady Europy dotycząca wzmocnienia ochrony whistle-blowerów.

USA

Początki whistleblowingu w USA datowane są od czasów wojny secesyjnej i do dziś w ramach whistleblowingu zewnętrznego i wewnętrznego miało miejsce wiele inicjatyw ustawodawczych, które w różnym zakresie chronić mają sygnalistów rozmaitych branż i sektorów w Stanach Zjednoczonych. Dla

sektora finansowego kluczowa miała być regulacja ustawy Sarbanes-Oxley Act[9], która nakazywała emitentom ustanowienie anonimowego whistleblowingu wraz z wynagrodzeniami za zgłoszenia. Jak się jednak okazało, na skutek stopnia skomplikowania procedury, rozkładu ciężaru dowodu i wykładni zawężającej tylko 3,6% wytoczonych spraw o ochronę whistleblowerów okazało się ich sukcesem[10]. Z tego właśnie powodu do kolejnej ustawy, tzw. Dodd-Frank Act[11], dodano sekcję 21F, która nie tylko wzmocniła ochronę sygnalistów przed stosowaniem represji ze strony pracodawcy, ale także w przypadku uzyskania tzw. oryginalnych informacji dała możliwość wynagradzania przez regulatora także anonimowych sygnalistów, w wysokości od 10 do 30% zasądzanej kary.

WIELKA BRYTANIA

Whistleblowing w Wielkiej Brytanii uregulowany jest co najmniej od lat 90. XX w., przy czym obecna ustawa, tzw. PIDA[12], uważana jest przez niektórych w wielu aspektach za wzorcową. Ustawa przewiduje możliwość whistleblowingu wewnętrznego i zewnętrznego do szerokiego spektrum adresatów, zapewnia ochronę nie tylko osobom zatrudnionym na umowę o pracę, stara się także wyważyć interesy przedsiębiorcy, wskazując obostrzenia w whistleblowingu zewnętrznym. Jednocześnie ustawa jako tzw. zgłoszenie kwalifikowane uznaje jedynie zgłoszenie poufne, czyli nieanonimowe, co z kolei wymaga większego zaufania do adresatów.

---

[9] An Act to protect investors by improving the accuracy and reliability of corporate disclosures made pursuant to the securities laws, and for other purposes (Sarbanes-Oxley Act), Pub. L. 107–204, 2002.

[10] R. E. Moberly, *Unfulfilled Expectations: An Empirical Analysis of Why Sarbanes-Oxley Whistleblowers Rarely Win*, 49 Wm. & Mary L. Rev. 65/2007, passim dostępny na http://scholarship.law.wm.edu/wmlr/vol49/iss1/3.

[11] An Act to promote the financial stability of the United States by improving accountability and transparency in the financial system, to end "too big to fail", to protect the American taxpayer by ending bailouts, to protect consumers from abusive financial services practices, and for other purposes (Dodd-Frank Act), Pub. L. 111–203, 2010.

[12] PIDA (Public Interest Disclosure Act 1998) An Act to protect individuals who make certain disclosures of information in the public interest; to allow such individuals to bring action in respect of victimisation; and for connected purposes, 1998 c. 23.

NIEMCY

W Niemczech brakuje kompleksowej regulacji odnośnie whistleblowingu, poza kilkoma regulacjami sektorowymi wynikającymi z dyrektyw UE (np. § 25a Abs. 1 Satz 6 Nr 3 Kreditwesengesetz, jako implementacja omówionej poniżej dyrektywy CRD IV). Sytuacji sygnalistów nie poprawia także orzecznictwo sądu pracy, które w ocenie ekspertów nie chroni w pełni zgłaszających naruszenia[13]. Z tego powodu za najważniejszą w kontekście ochrony sygnalistów uznaje się sprawę Heinisch vs Germany[14]. W 2011 r. Europejski Trybunał Praw Człowieka uznał, że niemieckie sądy krajowe nie wyważyły w odpowiedni sposób równowagi między potrzebą ochrony reputacji pracodawcy a potrzebą ochrony prawa do wyrażania opinii przez panią Heinische Brigitte – pielęgniarkę domu opieki, która zgłaszała liczne nieprawidłowości.

V. WHISTLEBLOWING ZGODNIE Z DYREKTYWĄ CRD IV I ROZPORZĄDZENIEM MAR

Prawodawstwo Unii Europejskiej nie doczekało się jednej, powszechnej regulacji odnośnie whistleblowingu, jednakże krok po kroku jest on regulowany w poszczególnych sektorach, w tym zwłaszcza w szeroko rozumianym sektorze finansowym. Z punktu widzenia banków najważniejsza jest dyrektywa CRD IV[15], dotycząca instytucji kredytowych, która została implementowana do polskiego porządku prawnego, oraz pakiet regulacji dotyczących przeciwdzia-

[13] G. Strack, *Whistleblowing in Germany*, [w:] *Whistleblowing: In defense*… op. cit., s. 109–125.

[14] ECTHR, Heinisch vs Germany, No 28274/08, 21.07.2011.

[15] 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).

łania nadużyciom na rynku, tj. dyrektywa MAD[16], rozporządzenie MAR[17] oraz dyrektywa wykonawcza do art. 32 tego rozporządzenia[18]. Zarówno dyrektywa CRD IV, jak i rozporządzenie MAR, wraz z dyrektywą wykonawczą, bardziej szczegółowo określają whistleblowing zewnętrzny, niemniej jednak obowiązek ustanowienia whistleblowingu wewnętrznego także określony jest wprost.

Artykuł 71 ust. 3 dyrektywy CRD IV

> Państwa członkowskie wymagają, by instytucje posiadały odpowiednie procedury zgłaszania przez swoich pracowników naruszeń wewnątrz firmy za pośrednictwem specjalnego, niezależnego i autonomicznego kanału.
>
> Takim kanałem mogą być również rozwiązania zapewniane przez partnerów społecznych. Zastosowanie ma taka sama ochrona, jak w przypadku ust. 2 lit. b), c) i d).

Artykuł 32 ust. 3 rozporządzenia MAR

> Państwa członkowskie wymagają, aby pracodawcy prowadzący działalność regulowaną przepisami w sprawie usług finansowych dysponowali odpowiednimi wewnętrznymi procedurami zgłaszania naruszeń niniejszego rozporządzenia przez ich pracowników.

O ile art. 71 ust. 3 dyrektywy CRD IV dotyczący „instytucji", tj. banków i firm inwestycyjnych, musiał zostać implementowany do porządku krajowego (odpowiednio art. 9 ust. 2a-2b ustawy – Prawo bankowe oraz art. 83a ust. 1a ustawy o obrocie instrumentami finansowymi), o tyle rozporządzenie MAR obowiązuje wprost. Jednak zakres przedmiotowy rozporządzenia MAR jest w stosunku do regulacji ustawy – Prawo bankowe o wiele węższy,

[16] Dyrektywa Parlamentu Europejskiego i Rady 2014/57/UE z dnia 16 kwietnia 2014 r. w sprawie sankcji karnych za nadużycia na rynku (dyrektywa w sprawie nadużyć na rynku) (Dz.U. UE L 173 z 12.06.2014 r., s. 179).

[17] Rozporządzenie Parlamentu Europejskiego i Rady (UE) NR 596/2014 z dnia 16 kwietnia 2014 r. w sprawie nadużyć na rynku (rozporządzenie w sprawie nadużyć na rynku) oraz uchylające dyrektywę 2003/6/WE Parlamentu Europejskiego i Rady i dyrektywy Komisji 2003/124/WE, 2003/125/WE i 2004/72/WE (Dz.U. UE L 173/1 z dnia 12.6.2014).

[18] Dyrektywa Wykonawcza Komisji (UE) 2015/2392 z dnia 17 grudnia 2015 r. w sprawie rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 596/2014 w odniesieniu do zgłaszania właściwym organom rzeczywistych lub potencjalnych naruszeń tego rozporządzenia (Dz.U. UE L332/26 z dnia 18.12.2015.

dotyczy bowiem jedynie *wykorzystywania informacji poufnych, bezprawnego ujawniania informacji poufnych i manipulacji na rynku (nadużyć na rynku)*, a więc istotnego, ale nie głównego przedmiotu działalności banków, zwłaszcza w Polsce. Z tego też względu niniejsze opracowanie odnosi się przede wszystkim do regulacji w ustawie – Prawo bankowe.

VI. WHISTLEBLOWING JAKO ELEMENT SYSTEMU ZARZĄDZANIA BANKIEM

Nowelizacja ustawy – Prawo bankowe, implementująca dyrektywę CRD IV, weszła w życie w dniu 1 listopada 2015 r.[19], co oznacza, że od tego momentu whistleblowing w bankach jest obowiązkowy. Zgodnie ze znowelizowanym brzmieniem art. 9 tej ustawy:

> Art. 9. 1. W banku funkcjonuje system zarządzania.
> 2. System zarządzania stanowi zbiór zasad i mechanizmów odnoszących się do procesów decyzyjnych, zachodzących w banku oraz do oceny prowadzonej działalności bankowej.
> 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.
> 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.
> 3. W ramach systemu zarządzania w banku funkcjonuje co najmniej:
> - system zarządzania ryzykiem,
> - system kontroli wewnętrznej.

[19] Ustawa z dnia 5 sierpnia 2015 r. o nadzorze makroostrożnościowym nad systemem finansowym i zarządzaniu kryzysowym w systemie finansowym (Dz.U. z 2015 r. poz. 1513).

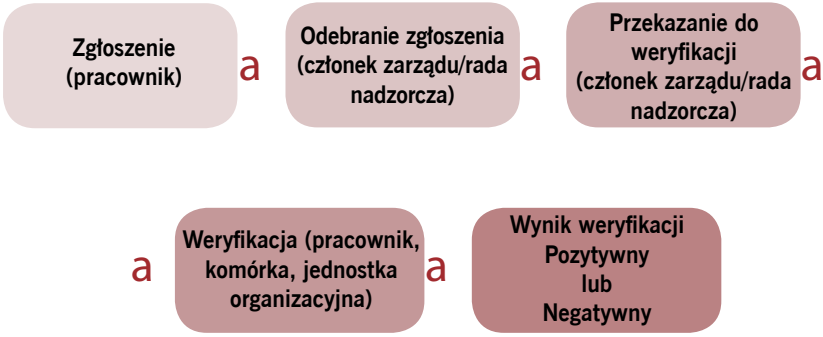
Ustawodawca milczy jednak w kwestii konkretyzacji wymogów w odniesieniu do whistleblowingu, delegując to zadanie na ministra właściwego do spraw instytucji finansowych, który zgodnie z art. 9f ustawy – Prawo bankowe określił je w drodze Rozporządzenia Ministra Rozwoju i Finansów z dnia 6 marca 2017 r. w sprawie systemu zarządzania ryzykiem i systemu kontroli wewnętrznej, polityki wynagrodzeń oraz szczegółowego sposobu szacowania kapitału wewnętrznego w banku (Dz.U. poz. 637) (dalej rozporządzenie MRiF). Rozdział 5 tego rozporządzenia dotyczący whistleblowingu wszedł w życie 1 maja 2017 r.

MIEJSCE WHISTLEBLOWINGU W SYSTEMIE ZARZĄDZANIA BANKIEM

Ustawodawca ustanawiając wymogi odnośnie whistleblowingu wskazuje, że ten ma być elementem systemu zarządzania *banku*, co oznacza, iż dotyczy to banku bez względu na formę prawną jego prowadzenia (bank w formie spółki akcyjnej, bank spółdzielczy, bank państwowy). Z kolei w art. 9 ust. 2a ustawy ustawodawca wskazał, iż „system zarządzania obejmuje procedury anonimowego zgłaszania…", a jednocześnie zachował w niezmienionej wersji art. 9 ust. 3 ustawy, zgodnie z którym „w ramach systemu zarządzania w banku funkcjonuje" co najmniej system zarządzania ryzykiem i system kontroli wewnętrznej. Wydawać by się mogło, że takie rozwiązanie dopuszcza przyporządkowanie whistleblowingu czy to do jednego z tych dwóch powyższych systemów (pasuje bardziej do systemu kontroli wewnętrznej), czy traktowania go jako odrębnego systemu bądź odrębne procedury. Jednakże skoro zgodnie z art. 9f ust. 1 pkt 1 ustawy „minister właściwy do spraw instytucji finansowych określi, w drodze rozporządzenia: szczegółowy sposób funkcjonowania w bankach systemu zarządzania ryzykiem i systemu kontroli wewnętrznej, w tym tryb anonimowego zgłaszania wskazanemu członkowi zarządu lub rady nadzorczej naruszeń prawa", wydaje się, że owe zgłaszanie powinno być wpisane w jeden z tych dwóch systemów. Wpisanie whistleblowingu w system zarządzania odgrywa kluczową rolę przy dopuszczalności outsourcingu, albowiem zgodnie z art. 6a ust. 3 pkt 1 ustawy, outsourcing zarządzania bankiem, w tym zwłaszcza zarządzania ryzykiem, jest niedopuszczalny.

PROCEDURY WHISTLEBLOWINGU W BANKU

Proces whistleblowingu według ustawy i rozporządzenia MRiF ilustruje poniższy rysunek:



Rysunek 1. Proces whistleblowingu w banku (oprac. wł.).

Schemat powyższego procesu należy, zgodnie z art. 9 ust. 2a ustawy, wpisać w procedury *anonimowego zgłaszania naruszeń.* Katalog minimum owych procedur, rozumianych jako „wszelkie akty wewnętrzne, w tym regulaminy, instrukcje, systemy i rozwiązania przyjęte w danym banku", został wprost wskazany w § 45 ust. 4 rozporządzenia MRiF i należy do niego co najmniej:

1) sposób odbierania zgłoszeń w sprawie naruszeń, zapewniający w szczególności możliwość odbierania zgłoszeń bez podawania tożsamości przez pracownika dokonującego zgłoszenia,

2) sposób ochrony pracownika dokonującego zgłoszenia, zapewniający co najmniej ochronę przed działaniami o charakterze represyjnym, dyskryminacją lub innymi rodzajami niesprawiedliwego traktowania,

3) sposób ochrony danych osobowych pracownika dokonującego zgłoszenia oraz osoby, której zarzuca się dokonanie naruszenia, zgodnie z przepisami ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. z 2016 r. poz. 922),

4) zasady zapewniające zachowanie poufności pracownikowi dokonującemu zgłoszenia, w przypadku gdy pracownik ten ujawnił swoją tożsamość lub jego tożsamość jest możliwa do ustalenia,

5) wskazanie osób odpowiedzialnych za odbieranie zgłoszeń naruszeń, z uwzględnieniem, że w przypadku gdy zgłoszenie dotyczy członka zarządu, powinno być ono przyjęte przez radę nadzorczą,

6) sposób przekazywania członkowi zarządu, o którym mowa w ust. 5, lub radzie nadzorczej oraz pracownikom, jednostkom organizacyjnym i komórkom organizacyjnym wyznaczonym zgodnie z ust. 6, informacji związanych ze zgłoszeniem naruszenia, niezbędnych do prawidłowej weryfikacji tego zgłoszenia, z uwzględnieniem ograniczenia zakresu przekazywanych informacji odpowiednio do celów realizowanych przez procedurę oraz treści zgłoszenia naruszenia,

7) rodzaj i charakter działań następczych podejmowanych na skutek:
   a) odebrania zgłoszenia naruszenia,
   b) weryfikacji zgłoszenia naruszenia
   – oraz sposób koordynacji tych działań,

8) termin usunięcia przez bank danych osobowych zawartych w zgłoszeniach naruszeń,

9) w przypadku pozytywnej weryfikacji zasadności zgłoszenia naruszenia termin powiadomienia przez członka zarządu wskazanego zgodnie z ust. 5 albo przez radę nadzorczą, gdy zgłoszenie dotyczy członka zarządu, osoby, której zarzuca się dokonanie naruszenia, o dokonanym zgłoszeniu naruszenia oraz o przeprowadzonej procedurze weryfikacji zasadności zgłoszenia naruszenia, z zastrzeżeniem zachowania poufności, o której mowa w pkt. 4.

ANONIMOWOŚĆ A POUFNOŚĆ WHISTLEBLOWINGU

Ustawodawca jednoznacznie przesądził, iż „System zarządzania obejmuje procedury anonimowego zgłaszania", co oznacza, iż „specjalny, niezależny i autonomiczny kanał" do zgłaszania naruszeń, o którym mowa w art. 71 ust.

3 dyrektywy CRD IV oraz § 45 ust. 3 rozporządzenia MRiF, służyć powinien do zgłaszania anonimowego. Nie oznacza to, jakoby ustawodawca zakazywał w ogóle zgłaszania poufnego (tj. pod nazwiskiem, ale bez możliwości ujawniania go przez otrzymującego zgłoszenie) czy bez zastrzegania poufności (np. przesyłanie uwag pod nazwiskiem poprzez skrzynkę e-mailową), ale takie zgłoszenia nie są już traktowane jako whistleblowing, a np. jako zgłaszanie skarg i wniosków przez pracowników.

Najbardziej oczywistym sposobem zapewnienia anonimowości jest udostępnienie pracownikom owego „specjalnego, niezależnego i autonomicznego kanału" do anonimowego korzystania, przy czym, wbrew pozorom, nie muszą to być technicznie zaawansowane narzędzia – przykładowo, zwykłe zabezpieczone skrzynki na pisemne wiadomości umieszczone tak, aby pracownicy bez obaw zidentyfikowania mogli składać zawiadomienia, zdają się realizować ten postulat. Niemniej takie rozwiązanie uniemożliwia późniejszy kontakt ze zgłaszającym w przypadkach gdy uściślenie informacji jest konieczne. Z tego też względu najpopularniejsze są kanały zgłoszeń online, które umożliwiają korespondencję nawet po anonimowym zgłoszeniu, gdy sygnalista, nie ujawniając tożsamości, może przesyłać dalsze informacje i zapytania[20]. Rodzi to jednak pytanie, czy zapewnienie anonimowości polegać ma jedynie na fizycznej niemożliwości ustalenia zgłaszającego, czy może nakłada na bank niejako obowiązek powstrzymywania się przed identyfikacją zgłaszającego za pomocą własnych systemów IT. Użyty w dyrektywie zwrot „specjalny, niezależny i autonomiczny kanał" przesądza, iż prawidłowe jest drugie z tych podejść, przy czym najbardziej wiarygodnym rozwiązaniem dla sygnalistów może być utrzymywanie takiego kanału przez podmiot zewnętrzny (np. na serwerach zewnętrznych poza bankiem). Takie rozwiązanie wymaga jednak szczególnej ostrożności w przypadku ochrony tajemnicy bankowej w outsourcingu IT.

ZAKRES, ADRESACI I AUTORZY ZGŁOSZEŃ

Zakres przedmiotowy zgłoszeń w ramach whistleblowingu dotyczy naruszeń prawa oraz obowiązujących w banku procedur i standardów etycznych. Tak szeroki katalog *de facto* kompleksowo obejmuje wszelkie możliwe naruszenia.

[20]Szerzej, patrz poradnik AICPA z 2010 r. dostępny na http://www.journalofaccountancy.com/news/2010/jun/auditcommitteeconsiderations.html.

Ustawodawca wskazał na „naruszania", a nie „podejrzenia naruszeń", tudzież „potencjalne naruszenia". Nie oznacza to jednak, iż zgłaszający musi mieć absolutną pewność, że doszło do popełnienia naruszeń, albowiem taką wiedzę można uzyskać dopiero po wnikliwym zbadaniu sprawy. Wystarczające powinno być uzasadnione podejrzenie, że w świetle wiedzy, którą dysponuje sygnalista, do naruszenia doszło.

Zgłaszającym (sygnalistą) może być każdy, ustawa nie wskazuje, kto może zgłaszać naruszenia, a jedynie komu bank ma zapewnić ochronę. Częstym i skutecznym źródłem są byli pracownicy, którzy dysponują kluczową wiedzą, pozwalającą przełamać asymetrię informacyjną. Zgodnie z opisanym powyżej nowym modelem whistleblowingu, ustawa nie wymaga także zgłoszenia w dobrej wierze, co oznacza, że powód zgłoszenia może być dowolny, kluczowa jest bowiem sama informacja i jej prawdziwość, a nie motywacja sygnalisty.

Adresatem zgłoszeń jest wskazany zgodnie z § 45 ust. 5 rozporządzenia MRiF członek zarządu, a w przypadku, gdy dotyczy to któregokolwiek z członków zarządu, jest nim, jak stanowi § 45 ust. 4 pkt 5 rozporządzenia MRiF, cała rada nadzorcza banku, a więc nie powinien to być ani komitet audytu, ani przewodniczący rady, a cała rada. Oznacza to również, iż bank, zgodnie z § 45 ust. 5 rozporządzenia MRiF, musi dokonać wewnętrznego podziału kompetencji, wskazując „członka zarządu, do którego są zgłaszane naruszenia oraz odpowiedzialnego za bieżące funkcjonowanie procedur anonimowego zgłaszania naruszeń". Ponadto „wewnętrzny podział kompetencji podlega zatwierdzeniu przez radę nadzorczą".

ROLA RADY NADZORCZEJ, ZARZĄDU I KOMÓREK ORGANIZACYJNYCH

Zgodnie z art. 9a ustawy – Prawo bankowe, zarząd banku projektuje, wprowadza oraz zapewnia działanie systemu zarządzania, zaś rada nadzorcza banku sprawuje nadzór nad wprowadzeniem systemu zarządzania oraz ocenia adekwatność i skuteczność tego systemu. Z racji przynależności whistleblowingu do systemu zarządzania bankiem, wskazane powyżej ogólne obowiązki dotyczą także whistleblowingu, które dodatkowo doprecyzowane są w art. 9 ust. 2a ustawy. Podział tych zadań nie różni się więc niczym od tradycyjnego

podziału ról między radą nadzorczą a zarządem, przy czym w ramach sprawowanego nadzoru rada nadzorcza, nie rzadziej niż raz na pół roku, otrzymuje informacje o otrzymanych istotnych zgłoszeniach naruszeń oraz w zależności od potrzeb, nie rzadziej niż raz w roku, ocenia adekwatność i skuteczność procedury anonimowego zgłaszania przez pracowników naruszeń. Ponadto, rolą rady nadzorczej jest stwierdzenie wewnętrznego podziału kompetencji, wskazującego członka zarządu, do którego są zgłaszane naruszenia oraz odpowiedzialnego za bieżące funkcjonowanie procedur anonimowego zgłaszania naruszeń.

Sytuacja zmienia się w przypadku, gdy naruszenie dotyczy jednego z członków zarządu. Wówczas dodatkowo rada nadzorcza obarczona jest obowiązkami analogicznymi do tych, które spoczywają na członku zarządu, o którym mowa w § 45 ust. 5 rozporządzenia MRiF. W zależności więc od tego, czy zgłoszenie dotyczy członka zarządu czy nie dotyczy, albo odpowiednio rada nadzorcza, albo członek zarządu, o którym mowa w § 45 ust. 5, mają obowiązek odebrania zgłoszenia, wyznaczenia podmiotów prowadzących weryfikację oraz poinformowania o fakcie dokonania zgłoszenia naruszenia, oraz przeprowadzonej procedurze weryfikacji. Zgodnie z § 45 ust. 6 rozporządzenia MRiF, ww. członek zarządu (albo rada nadzorcza, gdy zgłoszenie dotyczy członka zarządu) „po otrzymaniu zgłoszenia wyznacza pracowników, jednostki organizacyjne lub komórki organizacyjne odpowiedzialne za podejmowanie i koordynowanie weryfikacji zgłoszenia naruszenia oraz podejmowanie działań następczych". Oznacza to, że rodzaje i liczba wskazanych podmiotów mogą być dowolne (niekoniecznie musi to być jedna komórka), aczkolwiek wówczas należałoby wskazać podmiot koordynujący. Ponadto, nawet gdy w procedurze określono katalog komórek organizacyjnych przeprowadzających weryfikację, powinien on być katalogiem otwartym, tak żeby członek zarządu lub rada nadzorcza mogła wskazać inny podmiot, w szczególności gdy zgłoszenie dotyczyłoby pracowników właśnie tych komórek, które zwykle są wskazywane jako prowadzące weryfikację. Prawodawca milczy na temat rodzajów komórek, w praktyce wydaje się, że popularnymi rozwiązaniami są komórki tzw. drugiej linii obrony (zwłaszcza komórka do spraw zgodności), specjalne zespoły wyjaśniające, rzecznik etyki albo komisja etyczna.

VII. ZAKRES OCHRONY WHISTLEBLOWERÓW I PRZETWARZANIE DANYCH OSOBOWYCH

ZAKRES OCHRONY WHISTLEBLOWERÓW

Zgodnie z art. 9 ust. 2b ustawy – Prawo bankowe, w ramach procedur anonimowego zgłaszania naruszeń „bank zapewnia pracownikom, którzy zgłaszają naruszenia, ochronę co najmniej przed działaniami o charakterze represyjnym, dyskryminacją lub innymi rodzajami niesprawiedliwego traktowania". Ustawowe minimum oznacza także, że bank musi zapewnić ochronę pracownikom, a więc osobom związanym z bankiem stosunkiem pracy[21]. Wydaje się, że bank może dobrowolnie rozszerzyć taką ochronę również na pracowników związanych z bankiem umowami cywilnoprawnymi, ale także, co ważne w przypadku menadżerów, kontraktami menadżerskimi. Rodzą się jednak wątpliwości, skoro art. 9 ust. 2b ustawy wprost stanowi, iż bank zapewnia ochronę „w ramach procedur, o których mowa w ust. 2a", zaś ów ust. 2a mówi o „procedurach anonimowego zgłaszania", to czy oznacza to, iż ochronie podlegają tylko zgłaszający anonimowo, ale już nie np. poufnie. Wykładnia językowa jest jasna, niemniej wykładnia celowościowa z art. 71 ust. 2d dyrektywy CRD IV wskazuje, iż w przypadku whistleblowingu zewnętrznego ochronie podlegać powinni także zgłaszający w sposób poufny. Sygnaliści ci powinni bowiem podlegać ochronie „co najmniej przed działaniami o charakterze represyjnym, dyskryminacją lub innymi rodzajami niesprawiedliwego traktowania". Oznacza to, że decydujące będą przepisy, i co ważne, orzecznictwo antydyskryminacyjne z zakresu prawa pracy. Jak wskazuje w swoim opracowaniu Anna Wojciechowska-Nowak, w przypadku represji pracowników „pracodawcy często uciekali się do likwidacji stanowiska pracy, utraty zaufania do pracownika lub jego konfliktowego charakteru, a więc przyczyn,

[21] Szerzej patrz np. pismo KNF do prezesów Zarządów banków z dn. 12 grudnia 2012 r. (znak DPP/WOP1/023/663/2/2012/MS) odnośnie osób zatrudnionych w banku, o których mowa w art. 104 ust. 1 ustawy – Prawo bankowe.

które w sądzie pracy okazywały się trudne do podważenia"[22]. Ponadto, analizowane przez autorkę orzeczenia sądowe wskazywały, iż polscy sygnaliści „rzadko wygrywają w sądzie pracy, po drugie – sądy pracy, badając prawidłowość wypowiedzenia, najczęściej unikają odpowiedzi na pytanie, czy rozwiązanie stosunku pracy stanowiło formę odwetu za ujawnienie przez pracownika informacji o nieprawidłowościach"[23]. Przepisy ustawy – Prawo bankowe mają oczywiście przeciwdziałać takim sytuacjom. Z tego właśnie powodu samo wpisanie klauzuli o zapewnianiu ochrony w myśl art. 9 ust. 2b ustawy wydaje się niewystarczające, a banki powinny wskazać konkretne sytuacje/działania, jakich będą unikać w stosunku do pracownika w przypadku zgłaszania nieprawidłowości, gdyż mogą być uznane za działanie represyjne (np. zakaz przenoszenia na inne stanowisko pracy, zmiany warunków płacy i pracy, rozwiązania stosunku pracy etc.). Należy jednocześnie pamiętać, iż w kontekście prawa pracy w sprawach o dyskryminację to „pracodawca, chcąc zwolnić się z odpowiedzialności, musi udowodnić, że nie dyskryminuje pracownika"[24]. Z tego też powodu anonimowe procedury nie tylko chronią pracownika przed możliwością odwetu ze strony pracodawcy, ale i ułatwiają pracodawcy wykazanie, że np. zmieniając warunki płacy i pracy, nie stosuje odwetu. Nie zna przecież tożsamości sygnalisty. Należy jednak pamiętać, że samo anonimowe zgłoszenie nie zawsze musi oznaczać, że sygnalista nie zostanie, nawet mimowolnie, zidentyfikowany przez bank, albowiem sam może się przecież w dalszym toku ujawnić bądź przekazane informacje są na tyle unikalne, że trudno nie domyślić się, kto je przekazuje. W takim przypadku nadal jednak należy zapewnić zgłaszającemu poufność, o czym stanowi wprost § 45 ust. 4 pkt 4 rozporządzenia MRiF. Najtrudniejszym zagadnieniem odnośnie ochrony sygnalistów są przypadki, gdy sam sygnalista albo jest współuczestnikiem czy wręcz głównym sprawcą naruszenia, albo gdy świadomie zgłasza nieprawdę. Wydaje się, że w takim przypadku rozstrzygająca będzie interpretacja, co w takim kontekście oznaczają działania „o charakterze represyjnym, dyskryminacja lub inne rodzaje niesprawiedliwego traktowania". Ustawodawca, używając zwrotu „lub inne rodzaje niesprawiedliwego traktowania", jednoznacznie odwołał się do kryterium sprawiedliwości, a te trudno pogodzić z przypadkami umyślnego zgłaszania nieprawdy lub np. ciężkiego naruszenia obowiązków

[22] A. Wojciechowska-Nowak, *Jak zdemaskować szwindel? Czyli krótki przewodnik po whistleblowingu*, Fundacja Batorego, 2008.
[23] Ibidem, s. 18.
[24] Ibidem, s. 17.

pracowniczych. Kluczowa jednak, jak zawsze w takich przypadkach, będzie linia orzecznicza sądów pracy.

PRZETWARZANIE DANYCH OSOBOWYCH

Zagadnienie whistleblowingu budzi także wątpliwości w kontekście ustawy o ochronie danych osobowych[25]. Zgodnie z art. 25 ust. 1 tej ustawy w przypadku zbierania danych osobowych nie od osoby, której one dotyczą, administrator danych jest zobowiązany poinformować tę osobę, bezpośrednio po utrwaleniu zebranych danych, m.in.: o celu i zakresie zbierania danych, a w szczególności o odbiorcach lub kategoriach odbiorców danych, o źródle danych oraz prawie dostępu do treści swoich danych, oraz ich poprawiania. Konkretyzacja tego obowiązku nastąpiła w rozporządzeniu i uzależniona jest od tego, czy weryfikacja jest pozytywna (zgłoszenie się potwierdziło), czy negatywna (zgłoszenie się nie potwierdziło). Zgodnie z § 45 ust. 4 pkt 9 rozporządzenia MRiF, „w przypadku pozytywnej weryfikacji zasadności zgłoszenia naruszenia, termin powiadomienia przez członka zarządu wskazanego zgodnie z ust. 5, albo przez radę nadzorczą, gdy zgłoszenie dotyczy członka zarządu, osoby, której zarzuca się dokonanie naruszenia, o dokonanym zgłoszeniu naruszenia, oraz o przeprowadzonej procedurze weryfikacji zasadności zgłoszenia naruszenia, z zastrzeżeniem zachowania poufności, o której mowa w § 45 ust. 4 pkt 4".

Z kolei zgodnie z § 45 ust. 8 rozporządzenia MRiF, „w przypadku negatywnej weryfikacji zasadności zgłoszenia naruszenia i oddalenia podejrzeń w nim zawartych, członek zarządu wskazany zgodnie z ust. 5, albo rada nadzorcza, gdy zgłoszenie dotyczy członka zarządu, niezwłocznie powiadamiają osobę, której zarzucono dokonanie naruszenia, o dokonanym zgłoszeniu naruszenia oraz o przeprowadzonej procedurze weryfikacji zasadności zgłoszenia naruszenia, z zastrzeżeniem zachowania poufności, o której mowa w § 45 ust. 4 pkt 4".

Ponadto, zgodnie z § 45 ust. 9 rozporządzenia MRiF w przypadku weryfikacji negatywnej „bank niezwłocznie usuwa ze swoich systemów dane osobowe zawarte w zgłoszeniu, pozostawiając w systemach przez okres 5 lat, licząc od pierwszego dnia roku następującego po roku, w którym dokonano zgłoszenia,

[25] Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, Dz.U. z 2016 r. poz. 922.

inne informacje zawarte w zgłoszeniu naruszeń oraz informacje o podjętych działaniach następczych".

Dodatkową wskazówkę interpretacyjną może stanowić opinia tzw. Grupy Roboczej ds. ochrony danych powołanej na mocy art. 29 dyrektywy 95/46/WE[26], która w 2006 r., w oparciu o ówczesną dyrektywę, wydała poniższą opinię: „Zgodnie z art. 12 dyrektywy 95/46/WE osoba, której dane dotyczą, ma możliwość dostępu do danych zebranych na jej temat w celu sprawdzenia ich poprawności, skorygowania, jeśli są niepoprawne, niekompletne lub nieaktualne (prawo dostępu i sprostowania). W związku z tym system raportowania musi zapewniać osobom fizycznym prawo do dostępu do danych i prostowania niepoprawnych, niekompletnych lub nieaktualnych danych. Jednakże prawa te mogą zostać ograniczone w celu zapewnienia ochrony praw i swobód innych podmiotów objętych systemem. Ograniczenia tych praw powinny być rozpatrywane i nakładane indywidualnie. W żadnym wypadku, w ramach systemu i w oparciu o prawo dostępu osoby oskarżonej, osoba oskarżona w sprawozdaniu informatora nie może uzyskać informacji o jego tożsamości, z wyjątkiem przypadków, gdy informator, działając w złej woli, składa fałszywe oświadczenie. W każdym innym przypadku należy zapewnić anonimowość informatora"[27].

VIII. PODSUMOWANIE

Whistleblowing w bankach stanowi pierwszą tak kompleksową regulację ochrony sygnalistów w Polsce, co nie znaczy, że nie budzi ona żadnych interpretacyjnych wątpliwości. Wręcz przeciwnie, o ile bowiem sam sposób procedowania ze zgłoszeniami wydaje się dosyć jednoznaczny, aczkolwiek wymagający (np. aktywna rola rady nadzorczej przy zgłoszeniach dotyczących członka zarządu), to już faktyczny zakres ochrony whistleblowerów w dużej

[26] Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych OJ L 281, 23.11.1995, p. 31–50.

[27] Grupa robocza ds. ochrony danych powołana na mocy art. 29 dyrektywy 95/46/WE *Opinia 1/2006 w sprawie zastosowania unijnych zasad ochrony danych do wewnętrznych systemów informowania o nieprawidłowościach w dziedzinie księgowości, wewnętrznych kontroli księgowych, spraw związanych z audytem, zwalczania przekupstwa oraz przestępstw bankowych i finansowych*, 01.02.2006.

mierze zależny będzie od przyszłej wykładni sądowej. Niemniej należy mieć nadzieję, że te z rozwiązań przyjętych w whistleblowingu bankowym, które się w praktyce sprawdzą, będą powielane w kolejnych regulacjach tego typu, nie tylko w sektorze finansowym.

IX. LITERATURA

Banisar D., *Whistleblowing: International Standards and Developments*, [w:] Sandoval I., *Corruption and transparency: debating the frontiers between state, market and society*, World Bank-Institute for Social Research, UNAM, Washington 1.02.2011.

De George R. T., *Whistle-blowing*, NY Macmillan Publishing Company, Business Ethics 1986.

Hasink H., de Vries M., Bollen L., *A Content Analysis of Whistleblowing Policies of Leading European Companies*, "Journal of Business Ethics", 75/2007.

Hoffman W.M., McNulty R. E., *A business ethics theory of whistleblowing: responding to the $1 trillion question*, [w] Arszułowicz M., Gasparski W.W., *Whistleblowing: In defense of proper action*, *Praxiology: The International Annual of Practical Philosophy and Methodology*, Transaction Publishers, 2011.

Ionescu R., *Whistleblowing and disaster risk reduction*, [w:] Levis D., Vandekerckhove W., *Developments in Whistleblowing Research 2015*, Whistleblowing Research International Network 2015.

Jubb P. B., *Whistleblowing: A Restrictive Definition and Interpretation*, "Journal of Business Ethics" 21/1999.

Moberly R. E., *Unfulfilled Expectations: An Empirical Analysis of Why Sarbanes-Oxley Whistleblowers Rarely Win*, 49 Wm. & Mary L. Rev. 65 /2007.

Near J. P., Miceli M. P., *Organizational Dissidence: The Case of Whistleblowing*, "Journal of Business Ethics" 4/1985.

Strack G., *Whistleblowing in Germany*, [w:] Arszułowicz M., Gasparski W. W., *Whistleblowing: In defense of proper action*, *Praxiology: The International Annual of Practical Philosophy and Methodology*, Transaction Publishers, 2011.

Vandekerckhove W., *Whistleblowing and Organizational Social Responsibility: A Global Assessment*, Ashgate 2006.

KNF

CEDUR
Centrum Edukacji dla Uczestników Rynku

Komisja Nadzoru Finansowego
Pl. Powstańców Warszawy 1
Skr. poczt. nr 419, 00-950 Warszawa 1
Tel. (+48) 22 262 50 00
Fax (+48) 22 262 51 11
knf@knf.gov.pl
www.knf.gov.pl

ISBN 978-83-63380-17-5