Załącznik nr 1
do ZPZ No. C-I-70/24
z dnia 29.09.2024 r.

Procedura zgłaszania naruszeń w mBanku S.A.

§ 1
Wstęp

1. W mBanku nie akceptujemy łamania prawa, wymogów regulacyjnych, regulacji i zasad wewnętrznych ani jakiejkolwiek działalności przestępczej. Dlatego też mBank wspiera i chroni osoby zgłaszające naruszenia (dalej: sygnalista), zgodnie z zasadami, które opisuje ta procedura.
2. Celem wprowadzenia procedury jest zapobieganie nieprawidłowościom i zachęcenie sygnalistów do zgłaszania naruszeń prawa, standardów etycznych oraz regulacji wewnętrznych przyjętych w mBanku S.A.

§ 2
Definicje

1. **Bank** – mBank S.A, z siedzibą w Warszawie, ul. Prosta 18, 00-850 Warszawa, sąd rejestrowy: Sąd Rejonowy dla m. st. Warszawy XIII Wydział Gospodarczy Krajowego Rejestru Sądowego, KRS 0000025237, NIP: 526-021-50-88.
2. **DC** - Departament Compliance.
3. **Działanie następcze** – działanie, które podejmujemy w banku, aby ocenić prawdziwość informacji zawartych w zgłoszeniu oraz przeciwdziałać naruszeniu, które jest przedmiotem zgłoszenia, w szczególności przeprowadzamy postępowanie wyjaśniającego w trybie tej procedury.
4. **Działanie odwetowe** - bezpośrednie lub pośrednie działanie lub zaniechanie w kontekście związanym z pracą, które jest spowodowane zgłoszeniem i które narusza lub może naruszyć prawa sygnalisty lub wyrządza lub może wyrządzić nieuzasadnioną szkodę sygnaliście, w tym bezpodstawne inicjowanie postępowań przeciwko sygnaliście.
5. **Informacja zwrotna** - przekazana sygnaliście informacja na temat planowanych lub podjętych działań następczych i powodów takich działań.
6. **Kontekst związany z pracą** - przeszłe, obecne lub przyszłe działania związane z wykonywaniem pracy na podstawie stosunku pracy lub innego stosunku prawnego stanowiącego podstawę świadczenia pracy lub usług, w ramach których uzyskano informację o naruszeniu prawa oraz istnieje możliwość doświadczenia działań odwetowych.
7. **mSygnał** – aplikacja internetowa umożliwiająca zgłaszanie naruszeń online, imiennie lub anonimowo, 24 godziny na dobę, 7 dni w tygodniu.
8. **Naruszenie** – działanie lub zaniechanie niezgodne z prawem, regulacjami wewnętrznymi, standardami etycznymi banku lub mające na celu ich obejście.

9. **Naruszenie prawa** - działanie lub zaniechanie niezgodne z prawem lub mające na celu obejście prawa.
10. **Organ publiczny** - naczelne i centralne organy administracji rządowej, terenowe organy administracji rządowej, organy jednostek samorządu terytorialnego, inne organy państwowe oraz inne podmioty wykonujące z mocy prawa zadania z zakresu administracji publicznej.
11. **Osoba bliska** - małżonka / małżonek, wstępny / zstępny, inny krewny lub powinowaty, osoba pozostająca we wspólnym pożyciu; osoba pozostająca w stosunku przysposobienia, opieki lub kurateli; oraz osoba pozostająca we wspólnym gospodarstwie domowym.
12. **Osoba, której dotyczy zgłoszenie** – osoba, która została wskazana w zgłoszeniu jako ta, która dopuściła się naruszenia prawa, lub osoba, z którą ten naruszający prawo jest powiązany.
13. **Osoba pomagająca w zgłoszeniu** - osoba fizyczna, która pomaga sygnaliście w zgłoszeniu w kontekście związanym z pracą i której pomoc nie powinna zostać ujawniona.
14. **Osoba powiązana z sygnalistą** - osoba fizyczna, która może doświadczyć działań odwetowych, w tym współpracownik lub osoba najbliższa sygnalisty w rozumieniu art. 115 § 11 ustawy z dnia 6 czerwca 1997 r. – Kodeks karny (Dz. U. z 2024 r. poz. 17).
15. **RODO** - Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych).
16. **Sygnalista** - osoba fizyczna, która zgłasza informację o naruszeniu uzyskaną w kontekście związanym z pracą.
17. **Ustawa** - Ustawa z dnia 14 czerwca 2024 r. o ochronie sygnalistów.
18. **Zgłoszenie anonimowe** – przekazanie informacji o naruszeniu prawa przez osobę, która nie ujawniła swojej tożsamości i nie pozostawiła danych do kontaktu.
19. **Zgłoszenie wewnętrzne** - przekazanie bankowi informacji o naruszeniu.
20. **Zgłoszenie zewnętrzne** - przekazanie Rzecznikowi Praw Obywatelskich albo organowi publicznemu informacji o naruszeniu prawa.

§ 3
Informacje ogólne

1. Procedura ta określa tryb dokonywania zgłoszeń naruszeń w mBanku S.A., zasady ich weryfikacji i podejmowania działań naprawczych, a także ochrony sygnalisty.
2. Procedura ma zastosowanie do zgłaszanych naruszeń prawa w zakresie określonym w ustawie oraz obowiązujących w banku regulacji wewnętrznych i standardów etycznych.
3. Procedura nie zmienia zasad funkcjonowania innych kanałów przewidzianych dla zgłoszeń dotyczących innych tematów np. skarg i reklamacji klientów. W trybie procedury nie są obsługiwane przypadki nieprawidłowości, które zostały zidentyfikowane w wyniku kontroli wewnętrznej, rozpatrywania reklamacji klientów oraz zgłoszenia standardowych przypadków oszustw zewnętrznych, tj. oszustwa kartowe i kredytowe, phishing, które klienci lub inne osoby mogą zgłosić innymi kanałami, które funkcjonują w banku.
4. Przyjęte rozwiązania zapewniają, że zgłoszona sprawa zostanie zbadana przez niezależną jednostkę i sygnalista będzie podlegał ochronie. Nie wolno stosować jakichkolwiek form represji, dyskryminacji lub niesprawiedliwego traktowania wobec sygnalisty, który zgłasza podejrzenie popełnienia naruszenia, nawet wtedy, gdy podejrzenie nie zostanie

potwierdzone w toku postępowania wyjaśniającego. Wobec zgłaszającego nie mogą być podejmowane żadne działania odwetowe (**zasada ochrony sygnalisty**).

5. Wprowadzone przez bank kanały dla zgłoszeń wewnętrznych gwarantują ochronę tożsamości sygnalisty i osób trzecich wymienionych w zgłoszeniu oraz w razie potrzeby anonimowość. Informacje zamieszczone w zgłoszeniu jak też uzyskane w toku postępowania wyjaśniającego podlegają regulacjom o ochronie danych i należy je traktować jako poufne (**zasada poufności**).
6. Nie należy przekazywać informacji co do których zgłaszający miał pewność, że są nieprawdziwe w momencie dokonywania zgłoszenia (**zasada ochrony przed pomówieniem**).

§ 4
Sposoby zgłaszania naruszeń

1. Sygnalista może przekazać bankowi zgłoszenie naruszenia następującymi kanałami komunikacji:
   - **Elektronicznie** – za pośrednictwem aplikacji mSygnał, dostępnej na stronie internetowej banku: mSygnał**.**
   - **Korespondencyjnie**, pisemnie na adres: mBank, ul Prosta 18, 00-850 Warszawa, Departament Compliance WZN z dopiskiem „zgłoszenie naruszenia mBank – poufne”
2. Zgłoszenie można przekazywać imiennie lub anonimowo. W sytuacji, gdy pomimo zgłoszenia anonimowego, tożsamość zgłaszającego zostanie poznana na podstawie treści zgłoszenia lub podjętych czynności, podlega ona ochronie przewidzianej w procedurze.
3. Zgłoszenia naruszeń za pośrednictwem aplikacji mSygnał mogą być przekazywane w następujących kategoriach:
   a) korupcja,
   b) pranie pieniędzy/finansowanie terroryzmu,
   c) oszustwo,
   d) kradzież,
   e) nadużycia rynkowe/wykorzystanie informacji poufnych,
   f) sprzeniewierzenie/nadużycie zaufania,
   g) naruszenia wymogów regulacyjnych i przepisów prawa (w szczególności tych, które określa ustawa) oraz regulacji wewnętrznych banku,
   h) nieprawidłowości w stosunkach pracowniczych,
   i) naruszenie reguł etycznych.
4. Rekomendujemy zamieszczenie w zgłoszeniu poniższych informacji, według najlepszej wiedzy sygnalisty:
   a) gdzie miało miejsce naruszenie,
   b) kogo dotyczy zgłoszenie,
   c) kiedy się rozpoczęło/jak długo trwa naruszenie,
   d) szczegółowy opis zgłaszanego naruszenia,
   e) jaka jest relacja sygnalisty z bankiem,
   f) szacowana kwota ewentualnej straty,
   g) wszelkie dowody i informacje, które mogą być przydatne do weryfikacji naruszenia.
5. Zachęcamy do podania danych kontaktowych. Podanie adresu do kontaktu do korespondencji w formie papierowej nie ma zastosowania do zgłoszeń anonimowych. W

przypadku zgłoszenia za pośrednictwem aplikacji mSygnał, sygnalista może utworzyć anonimową skrzynkę do kontaktu.

§ 5
Tryb rozpatrywania zgłoszeń wewnętrznych

1. Bezpośredni dostęp do wszystkich zarejestrowanych zgłoszeń naruszeń ma wyznaczony członek Zarządu oraz upoważnieni pracownicy DC zatrudnieni na stanowisku ds. przeciwdziałania nadużyciom i korupcji.
2. DC jest jednostką upoważnioną do przyjmowania i weryfikacji zgłoszeń wewnętrznych, podejmowania działań następczych i prowadzenia komunikacji z sygnalistą.
3. Ze względu na zakres odpowiedzialności i wymaganą wiedzę merytoryczną zgłoszenia mogą być obsługiwane przez upoważnionych pracowników, innych niż DC jednostek banku, którzy rozpatrują je wg kategorii i zgodnie ze swoimi kompetencjami i regulacjami wewnętrznymi banku z zachowaniem zasad i terminów określonych w tej procedurze.
4. Zgłoszenie wewnętrzne nie może być obsługiwane na żadnym etapie przez pracownika, którego dotyczy zgłoszenie, lub co do którego zachodzą uzasadnione przesłanki braku bezstronności lub niezależności, w szczególności jeśli jest osobą bliską dla sygnalisty lub osoby której dotyczy zgłoszenie.
5. DC odpowiada za koordynowanie oraz monitorowanie terminowości rozpatrywania zgłoszeń przez pracowników innych jednostek organizacyjnych.
6. Upoważniony pracownik, który podejmuje zgłoszenie, analizuje czy dotyczy ono naruszenia w rozumieniu procedury oraz czy zawiera informacje wystarczające do przeprowadzenia dalszego postępowania wyjaśniającego. Jeżeli wynik analizy jest pozytywny, rozpoczyna postępowanie wyjaśniające w celu weryfikacji treści zgłoszenia. W przypadku jeżeli wynik analizy jest negatywny zamyka zgłoszenie jako niepotwierdzone.
7. Upoważniony pracownik w terminie do 7 dni od otrzymania zgłoszenia potwierdza sygnaliście przyjęcie zgłoszenia i zawiadamia o rozpoczęciu postępowania wyjaśniającego lub informuje go, że zgłoszenie zostało zamknięte (podając przyczynę) lub zakwalifikowane jako reklamacja, może też prosić o dodatkowe informacje. Pracownik, kontaktuje się z sygnalistą w taki sposób, jaki sygnalista wskazał w zgłoszeniu.
8. Upoważnieni pracownicy przeprowadzają postępowania wyjaśniające i podejmują działania następcze, z zachowaniem należytej staranności, w celu ustalenia stanu faktycznego i wyjaśnienia wszystkich wątpliwości dotyczących sytuacji opisanej w zgłoszeniu. Zbierają dowody, które pozwolą na rozpatrzenie zgłoszenia naruszenia w sposób obiektywny, sumiennie i bezstronnie.
9. Upoważniony pracownik przekazuje zgłaszającemu informację zwrotną o przeprowadzonym postępowaniu wyjaśniającym nie później niż w ciągu 3 miesięcy od dnia potwierdzenia przyjęcia zgłoszenia wewnętrznego.
10. Zapisów ust. 7 i 9 nie stosujemy, jeśli sygnalista nie utworzył skrzynki w aplikacji mSygnał ani nie wskazał adresu do kontaktu, na który należy przekazać informację zwrotną.

§ 6
Zgłoszenie zewnętrzne

1. Sygnalista ma prawo do dokonania zgłoszenia zewnętrznego do Rzecznika Praw Obywatelskich, organów publicznych oraz – w stosownych przypadkach – do instytucji,

organów lub jednostek organizacyjnych Unii Europejskiej, zgodnie z odpowiednimi przepisami prawa.

2. Sygnalista może dokonać zgłoszenia zewnętrznego bez uprzedniego dokonania zgłoszenia wewnętrznego. Bank zachęca jednakże do przekazywania informacji o naruszeniach za pośrednictwem wewnętrznych kanałów w trybie niniejszej procedury, aby móc skutecznie reagować na nieprawidłowości i zapobiegać ich występowaniu w przyszłości.
3. Dokonanie zgłoszenia zewnętrznego nie pozbawia sygnalisty prawa do ochrony przed działaniami odwetowymi.
4. Szczegółowe zasady dokonywania, rozpatrywania i ochrony dla trybu zgłoszenia zewnętrznego określa w ustawa.

§ 7
Ochrona sygnalisty

1. Bank umożliwia zgłaszanie naruszeń w sposób zapewniający zgłaszającemu ochronę przed działaniami odwetowymi. Wobec sygnalisty nie mogą być podejmowane żadne działania odwetowe ani próby lub groźby zastosowania takich działań.
2. Ochrona przed działaniami odwetowymi obejmuje sygnalistę, osoby pomagające mu w dokonaniu zgłoszenia oraz osoby powiązane z sygnalistą. Zakaz działań odwetowych i środki ochrony dotyczą też osoby prawnej lub innej jednostki organizacyjnej pomagającej sygnaliście lub z nim powiązanej, w szczególności stanowiącej własność sygnalisty lub go zatrudniającej.
3. Sygnalista podlega ochronie od chwili dokonania zgłoszenia, pod warunkiem, że miał uzasadnione podstawy sądzić, że informacje zawarte w zgłoszeniu są prawdziwe w momencie dokonywania zgłoszenia i że stanowią informacje o naruszeniu prawa lub standardów etycznych/regulacji wewnętrznych banku.
4. Zakaz działań odwetowych obowiązuje także, jeżeli w wyniku postępowania wyjaśniającego okaże się, że naruszenie było zgłoszone w dobrej wierze, a ostatecznie nie zostało potwierdzone.
5. Sygnalista, w stosunku do którego zastosowano działania odwetowe powinien niezwłocznie powiadomić o zaistniałej sytuacji pracownika banku udostępnionymi kanałami komunikacji dla zgłoszeń wewnętrznych. Zgłoszenie zostanie wyjaśnione w trybie przewidzianym dla zgłoszeń wewnętrznych.
6. Sygnalista, wobec którego dopuszczono się działań odwetowych, ma prawo do odszkodowania w wysokości nie niższej niż przeciętne miesięczne wynagrodzenie w gospodarce narodowej w poprzednim roku, ogłaszane do celów emerytalnych w Dzienniku Urzędowym Rzeczypospolitej Polskiej „Monitor Polski” przez Prezesa Głównego Urzędu Statystycznego, lub prawo do zadośćuczynienia.
7. Osoba, która poniosła szkodę z powodu świadomego zgłoszenia nieprawdziwych informacji przez sygnalistę, ma prawo do odszkodowania lub zadośćuczynienia za naruszenie dóbr osobistych od sygnalisty, który dokonał takiego zgłoszenia.
8. Dokonanie zgłoszenia nie może stanowić podstawy odpowiedzialności, w tym odpowiedzialności dyscyplinarnej lub odpowiedzialności za szkodę z tytułu naruszenia praw innych osób lub obowiązków określonych w przepisach prawa pod warunkiem, że sygnalista miał uzasadnione podstawy sądzić, że zgłoszenie jest niezbędne do ujawnienia naruszenia prawa.

§ 8
Poufność

1. Bank zapewnia, że przyjęty tryb obsługi zgłoszeń wewnętrznych oraz związane z tym przetwarzanie danych osobowych uniemożliwiają nieupoważnionym osobom uzyskanie dostępu do informacji objętych zgłoszeniem oraz zapewniają ochronę poufności tożsamości sygnalisty, osoby, której dotyczy zgłoszenie, oraz osoby trzeciej wskazanej w zgłoszeniu. Ochrona poufności dotyczy informacji, na podstawie których można bezpośrednio lub pośrednio zidentyfikować tożsamość takich osób.
2. Zgromadzone informacje, które dotyczą zgłoszenia wewnętrznego, podlegają ochronie i dostęp do nich mogą mieć tylko osoby upoważnione do przyjmowania i weryfikacji zgłoszeń wewnętrznych, podejmowania działań następczych oraz przetwarzania danych osobowych sygnalisty, osoby, której dotyczy zgłoszenie, oraz osoby trzeciej wskazanej w zgłoszeniu naruszenia. Z wyjątkiem sytuacji, w których konieczność udostępnienia informacji wynika z powszechnie obowiązujących przepisów prawa.
3. Upoważnione osoby, które obsługują zgłoszenia wewnętrzne są zobowiązane do zachowania tajemnicy odnośnie do informacji i danych osobowych, które uzyskały w ramach przyjmowania i weryfikacji zgłoszeń, oraz podejmowania działań następczych, także po ustaniu stosunku pracy lub innego stosunku prawnego, w ramach którego wykonywały tę pracę.
4. W przypadku zgłoszenia anonimowego nie wolno podejmować jakichkolwiek działań mających na celu zidentyfikowanie tożsamości sygnalisty.

§ 9
Przetwarzanie danych osobowych

1. Wszelkie dane osobowe pozyskane w związku ze zgłoszeniami wewnętrznymi naruszeń w trybie określonym w tej procedurze są przetwarzane zgodnie z postanowieniami RODO oraz innych powszechnie obowiązujących przepisów prawa oraz regulacji wewnętrznych banku.
2. Bank po otrzymaniu zgłoszenia przetwarza dane osobowe w zakresie niezbędnym do przyjęcia zgłoszenia lub podjęcia ewentualnego działania następczego. Dane osobowe, które nie mają znaczenia dla rozpatrywania zgłoszenia, nie są zbierane, a w razie przypadkowego zebrania są niezwłocznie usuwane. Usunięcie tych danych osobowych następuje w terminie 14 dni od chwili ustalenia, że nie mają one znaczenia dla sprawy.
3. Dane osobowe sygnalisty, pozwalające na ustalenie jego tożsamości, nie podlegają ujawnieniu nieupoważnionym osobom, chyba że za wyraźną zgodą sygnalisty. Zasady tej nie stosuje się w przypadku, gdy ujawnienie jest koniecznym i proporcjonalnym obowiązkiem wynikającym z przepisów prawa w związku z postępowaniami wyjaśniającymi prowadzonymi przez organy publiczne lub postępowaniami przygotowawczymi lub sądowymi prowadzonymi przez sądy.
4. Dane osobowe przetwarzane w związku ze zgłoszeniem wewnętrznym lub podjęciem działań następczych oraz dokumenty związane z tym zgłoszeniem są przechowywane przez okres 3 lat po zakończeniu roku kalendarzowego, w którym zakończono działania następcze, lub po zakończeniu postępowań sądowych zainicjowanych tymi działaniami.
5. Dane osobowe oraz pozostałe informacje w rejestrze zgłoszeń wewnętrznych są przechowywane przez okres 3 lat po zakończeniu roku kalendarzowego, w którym

zakończono działania następcze, lub po zakończeniu postępowań zainicjowanych tymi działaniami chyba, że obowiązujące przepisy prawa przewidują inne terminy przechowywania i usuwania informacji.

§ 10
Postanowienia końcowe

1. Bank regularnie dokonuje przeglądu zasad określonych w tej procedurze (przynajmniej co 12 miesięcy) i w razie potrzeby odpowiednio je aktualizuje.
2. Procedura jest publikowana na stronie internetowej banku.