ПРИВАТНЕ АКЦІОНЕРНЕ ТОВАРИСТВО
«СТРАХОВА КОМПАНІЯ «АХА СТРАХУВАННЯ»

«ЗАТВЕРДЖЕНО»

Наказом Голови Правління
АТ «СК «АХА Страхування»
№ 19-О від 31.01.2017р.

ПОЛОЖЕННЯ ПРО ПОДАЧУ ПОВІДОМЛЕНЬ ПРО ПОРУШЕННЯ

(НОВА РЕДАКЦІЯ)

м. Київ, 2017 р.

1. ЗАГАЛЬНІ ПОЛОЖЕННЯ

1.1. Положення про подачу повідомлень про порушення розроблено та затверджено в рамках ініціатив, заходів та дій, що вживаються АТ «СК «АХА Страхування» (далі - «Компанія») і її керівництвом для ефективної протидії зловживанням, своєчасного виявлення можливих фактів корупції, шахрайства або неправомірного заволодіння, розголошення та/або використання інформації, що становить комерційну таємницю, чи інших порушень у діяльності Компанії.

1.2. Положення про подачу повідомлень про порушення поширюється на всіх співробітників Компанії.

2. ЦІЛІ І ПРИНЦИПИ ПОДАЧІ ПОВІДОМЛЕНЬ ПРО ПОРУШЕННЯ

2.1. Цілі подачі повідомлень про порушення

Співробітники Компанії, а також інші особи (звільнені співробітники Компанії, представники клієнтів, посередників, постачальників та ін.) (разом далі - «Відправники», а окремо - «Відправник») мають право в рамках цього Положення подати повідомлення (далі – «повідомлення про порушення») про:

- ✓ Шахрайські дії, скоєні співробітниками Компанії, в тому числі, розкрадання, зловживання активами, корупційні та інші дії, що негативно впливають на збереження активів Компанії, у тому числі баз даних клієнтів;
- ✓ Корупцію та зловживання службовим становищем;
- ✓ Порушення співробітниками Компанії етичних норм, наприклад: робота на конкурентів, конфлікти інтересів, отримання подарунків, що впливають або створюють враження таких, що впливають на рішення співробітника Компанії при виконанні ним своїх службових обов'язків, розголошення конфіденційної інформації, тощо;
- ✓ Порушення у сфері трудових відносин та управління персоналом, наприклад: домагання, дискримінація, неадекватна поведінка на робочому місці, потенційні порушення законодавства про працю;
- ✓ Фальсифікацію фінансової звітності;
- ✓ Фальсифікацію іншої звітності, наприклад: у сфері управління персоналом, стратегічному плануванні, продажах, управління активами тощо;
- ✓ Інші порушення співробітниками Компанії чинного законодавства, в тому числі антимонопольного чи про запобігання недобросовісній конкуренції, легалізації (відмиванню) доходів, одержаних злочинним шляхом чи фінансуванню тероризму тощо;
- ✓ Інші дії співробітників Компанії, здатні призвести до виникнення у Компанії фінансових втрат або зашкодити її репутації, і дії іншого характеру, що йдуть врозріз з її інтересами.

2.2. Недопустимі цілі подачі повідомлень про порушення

2.2.1. Не допускається подача повідомлення про порушення для:

- ✓ Поширення завідомо неправдивих відомостей, наклепів тощо;
- ✓ Зведення особистих рахунків, досягнення особистих цілей, що суперечать інтересам Компанії;

- ✓ Образи, вираження загроз життю і здоров'ю співробітників Компанії або їх близьких осіб і родичів.

2.2.2. Відповідальні особи Компанії, що забезпечують прийом і обробку повідомлень про порушення, залишають за собою право за результатами первинної перевірки не брати до уваги повідомлення та інформацію, які явно не належать до цілей цього Положення, а також вживати дозволені законодавством заходи стосовно повідомлень та інформації, переданих з явно несумлінними, наклепницькими або протизаконними намірами.

2.3. **Канали і способи передачі повідомлень**

2.3.1. У разі виявлення факту вчинення або наявності достатніх підстав для підозр у вчиненні порушень, передбачених у п. 2.1 співробітнику Компанії рекомендується повідомляти про них в звичайному порядку підлеглості, тобто своєму безпосередньому керівнику.

2.3.2. При цьому такий керівник, як і будь-який співробітник Компанії, який отримав таке повідомлення, зобов'язані негайно повідомити про це Менеджера з протидії шахрайству.

2.3.3. Співробітник Компанії, який вважає недоцільним, з урахуванням обставин, повідомляти про порушення, зазначені у п. 2.1 безпосередньому керівнику, може одразу надіслати повідомлення Менеджеру з протидії шахрайству використовуючи наступні канали зв'язку:

- ✓ електронну адресу ***anti-fraud@axa-ukraine.com***;
- ✓ форму, розміщену на офіційному веб-сайті Компанії в розділі «Компанія» - «AXA в Україні» - «Повідомити про порушення www.axa-ukraine.com/company/axa-in-ukraine/submit-whistleblower-report;
- ✓ автовідповідач (067) 506-62-50;
- ✓ факс (067) 560-77-14;
- ✓ поштову адресу: 04070, м. Київ, вул. Іллінська 8 з відміткою «Повідомлення про порушення» або «Для менеджера з протидії шахрайству», або «Начальнику управління внутрішнього аудиту» При цьому, такі листи не дозволяється відкривати у процесу обробки кореспонденції що надходить до Компанії.

2.3.4. Менеджер з протидії шахрайству контролює, щоб по всім повідомленням, які є сумлінними і містять достатньо інформації для їх оцінки, була ініційована службова перевірка. Менеджера з протидії шахрайству та Начальник управління внутрішнього аудиту повинні мати доступи необхідні, для отримання ними усіх без винятку повідомлень про порушення надісланими усіма каналами зв'язку.

2.3.5. Для тих співробітників, які побоюються, що Компанія може вживати заходів технічного характеру для встановлення їх IP-адресів та/або не впевнені, що їх повідомлення не будуть проігноровані Менеджером з протидії шахрайству, існує можливість надіслати повідомлення про порушення, передбачені у п. 2.1, ***Представнику Групи AXA та Голові аудиторського комітету Наглядової Ради Компанії - Alex PEJOUX*** (далі – Контактна особа Групи) на його електронну адресу ***alexandre.pejoux@axa-lifeinvest.com***;

При отриманні таких повідомлень Контактна особа Групи:

- ✓ видаляє будь-які дані про Відправника, зокрема його електронну адресу;
- ✓ пересилає повідомлення Менеджеру з протидії шахрайству для подальшого розгляду та реагування;

- ✓ контролює процес розгляду та реагування на таке повідомлення з боку Менеджера з протидії шахрайству особи.

Таким чином, забезпечується додаткова анонімність особистості Відправника і незалежний контроль над ходом розгляду повідомлення Менеджером з протидії шахрайству .

2.4. **Формат повідомлень**

2.4.1. Повідомлення можуть бути надані Відправником у будь-якому зручному для нього форматі.

2.4.2. Однак, з метою ефективної обробки повідомлень, що надходять, рекомендується зазначати в них такі відомості:

- ✓ найменування структурного або відокремленого підрозділу, про який йде мова в повідомленні;
- ✓ дату і час порушення/події, про яке йде мова в повідомленні, або часовий період, у разі якщо порушення мало повторюваний/триваючий характер;
- ✓ ПІБ та/або посаду порушника/співробітника, відповідального за належне виконання обов'язків, що є предметом повідомлення;
- ✓ стислий опис порушення/події (у тому числі, конкретні суттєві факти і обставини, значущі подробиці, можливі причини);
- ✓ можливі наслідки порушення/події та/або збиток, нанесений Компанії, про які відомо Відправникові;
- ✓ чи повідомляв Відправник будь-яку інформацію про порушення кому-небудь в Компанії або третім особам (якщо так, то необхідно вказати їх ПІБ та посаду, а також результат розгляду/обговорення);
- ✓ ПІБ та/або посаду співробітників Компанії, які можуть знати про порушення/подію і підтвердити або доповнити інформацію, що повідомляється;
- ✓ при бажанні (для зворотного зв'язку) - персональні дані Відправника: контактний номер телефону, посаду або ПІБ.

2.5. **Анонімне надання повідомлень**

2.5.1. Відправник має право зберігати анонімність при подачі повідомлень про порушення.

2.5.2. Однак Відправники, які анонімно надали повідомлення, повинні усвідомлювати складність подальшого розгляду таких повідомлень і можливого проведення службового розслідування по зверненню, яке надійшло від них, оскільки відсутня можливість уточнення отриманої інформації та надання зворотного зв'язку.

2.5.3. На ступінь реального захисту Вашої анонімності в першу чергу впливають Ваші власні дії при відправці повідомлень, а також дотримання зазначених нижче рекомендацій, які повинні забезпечити повну анонімність при Вашому бажанні:

✓ **електронний лист** – скористайтеся будь-якою публічною поштовою скринькою на загальнодоступних серверах електронної пошти, через інтернет-кафе або з будь-якого іншого місця, які не вимагають обов'язкової реєстрації користувачів або не використовують алгоритми посвідчення Вашої особистості; не підписуйте Ваше повідомлення;

✓ **офіційний веб-сайт Компанії** – приховайте свою IP-адресу використовуючи проксі (проміжний сервер). Замість того, щоб заходити на сайт безпосередньо, Ви можете

використовувати проксі-сервер, у цьому випадку очевидним є лише Ваш зв'язок з проміжним проксі-сервером.

Для цього можна скористатися будь-яким сайтом-анонімайзером, наприклад, http://anonymouse.org.

Є й інший варіант маскування IP-адреса. Користувачі інтернет-браузера Firefox можуть перейти на безкоштовний інтернет-браузер xB-Browser (http://xb-browser.ru.uptodown.com), відомий раніше під назвою Torpark, який представляє собою модифіковану версію браузера Firefox. А ті, хто в якості інтернет-браузера надає перевагу Opera, — можуть скористатися програмною зв`язкою OperaTor (http://soft.oszone.net/program/4533/OperaTor), що включає, крім браузера, клієнт анонімної мережі Tor і віртуальний проксі-сервер Polipo. В обох варіантах всі запитані при серфінгу дані передаватимуться не безпосередньо, а через мережу анонімної передачі даних TOR. У цій мережі пакети пересилаються по випадкових маршрутах через декілька серверів (маршрути кожну хвилину міняються), причому сервери використовують зашифровані з'єднання і приховують всі сліди пересилки інформації.

Для регулярної анонімної роботи можна використовувати програму TOR (https://www.torproject.org). Це інструмент, який автоматично вибирає для Вас працюючі проксі-сервера.

- ✓ **голосове повідомлення** – не називайте себе, Ваш підрозділ, Вашого керівника або інші деталі в повідомленні, які можуть прямо або опосередковано сприяти визначенню Вашої особистості; не використовуйте для дзвінків Ваш службовий, домашній, мобільний чи інші телефони, за номером яких Вас можна визначити;
- ✓ **звичайний лист/факс** – не підписуйте лист Вашим ім'ям; не вказуйте в ньому деталі, які можуть прямо або опосередковано сприяти визначенню Вашої особистості; не відправляйте лист через кур'єра, якщо це може призвести до визначення відправника, використовуйте публічні місця і пошту для відправки кореспонденції.

3. ГАРАНТІЇ БЕЗПЕКИ У ЗВ'ЯЗКУ З ПОДАЧЕЮ ПОВІДОМЛЕНЬ ПРО ПОРУШЕННЯ

3.1. Гарантія конфіденційності

3.1.1. Компанія, в рамках своїх повноважень і наявних можливостей, забезпечує конфіденційність інформації про особу Відправника, який із сумлінними намірами надав інформацію про порушення, зазначені п. 2.1 цього Положення.

Менеджер з протидії шахрайству, Контактна особа Групи, інші особи, які беруть участь у розгляді та реагуванні на Повідомлення, зокрема, Начальник управління внутрішнього аудиту та члени Правління та директора відповідних департаментів, не мають права розкривати зазначену інформацію іншим співробітникам Компанії або третім особам, за винятком випадків, передбачених чинним законодавством.

3.1.2. Однак Компанія не несе відповідальність за збереження конфіденційності інформації про особу Відправника, якщо він добровільно, в тому числі з необережності, розкриває факт подачі повідомлення про порушення іншим співробітникам Компанії або третім особам.

3.1.3. З метою забезпечення конфіденційності інформації про особу Відправника повідомлення передаються Менеджером з протидії шахрайству для перевірки/розслідування та підготовки відповіді без зазначення персональних даних Відправника.

3.2. Відмова від переслідування Відправників

3.2.1. Забороняється переслідування Відправника з боку Компанії у зв'язку з подачею ним повідомлення про порушення, за винятком випадків, передбачених чинним законодавством.

Компанія гарантує, що Відправники, які сумлінно повідомили про порушення інших співробітників Компанії, не будуть піддані санкціям, у тому числі звільнені, понижені в посаді, позбавлені премії тощо.

3.2.2. При цьому Компанія залишає за собою право притягнути Відправника, що надав завідомо неправдиву інформацію, до відповідальності згідно із чинним законодавством та внутрішніми документами Компанії.

4. ПОРЯДОК РОЗГЛЯДУ ПОВІДОМЛЕНЬ ТА НАДАННЯ ВІДПОВІДЕЙ

4.1.1. Компанія прагне забезпечити довіру співробітників і відкритий діалог з ними шляхом своєчасного та об'єктивного розгляду всіх повідомлень, що надійшли без урахування посадового становища та стажу роботи в Компанії співробітника, стосовно якого надійшло повідомлення.

4.1.2. Після отримання повідомлення Менеджер з протидії шахрайству проводить його аналіз. Якщо повідомлення є недобросовісним або якщо наявної інформації недостатньо для його оцінки, подальший його розгляд не проводиться, а службова перевірка не ініціюється. Всі сумлінні повідомлення, що мають достатньо інформації для їх оцінки підлягають розслідуванню в рамках службової перевірки.

4.1.3. Службову перевірку ініціює Менеджер з протидії шахрайству після консультацій з Головою Правління та Начальником управління внутрішнього аудиту, а при необхідності з відповідним Заступником Голови Правління, у вертикалі якого працює співробітник, стосовно якого надійшло повідомлення, крім випадків, обумовлених цим Положенням. Якщо повідомлення надійшло стосовно членів або Голови Правління консультації проводяться з Головою кластеру AXA Emerging Europe.

4.1.4. До проведення службової перевірки, крім випадків обумовлених даним Положенням, обов'язково залучається керівник керівника співробітника, стосовно якого надійшло звернення. Якщо повідомлення надійшло стосовно Голови Правління, його Заступників, Фінансового директора, Головного актуарія, Директора Департаменту ризик-менеджменту, Начальника управління внутрішнього аудиту або Управління нормативного контролю та фінансового моніторингу до проведення службової перевірки залучається Офіс Голови Групи AXA.

4.1.5. Співробітник Компанії не може брати участь в ініціюванні або проведенні службової перевірки, якщо повідомлення стосується його особисто та/або можливий конфлікт інтересів.

4.1.6. При проведенні службової перевірки аналізуються факти, що спричинили виникнення проблем, і вживаються заходи щодо їх запобігання в майбутньому.

4.1.7. В ході службової перевірки з'ясовуються наступні питання:

- ✓ коли, де і якими засобами був здійснений службовий проступок;
- ✓ хто вчинив службовий проступок;
- ✓ які обставини і причини привели до скоєння проступку;
- ✓ чи є в скоєному проступку ознаки адміністративного правопорушення або кримінального злочину;
- ✓ наявність обставин, що пом'якшують або обтяжують відповідальність винної особи;
- ✓ розмір збитку, заподіяний Компанії;

4.1.8. В ході службової перевірки про неї в межах доцільності повідомляється співробітник Компанії, стосовно якого надійшло повідомлення, якому надається можливість дати пояснення за обставинами справи.

4.1.9. За результатами перевірки Менеджер з протидії шахрайству, за наявності такої можливості, може сповістити Відправника повідомлення про результати перевірки та вжитих

заходах (якщо Відправник побажав отримати таке повідомлення і залишив контактну інформацію).

5. ОБЛІК І ЗВІТНІСТЬ

5.1.1. Менеджер з протидії шахрайству веде реєстр отриманих повідомлень, підтримує його в актуальному стані, в тому числі регулярно оновлюючи статус розгляду таких повідомлень.

5.1.2. Кожному повідомленню в реєстрі присвоюється окремий ідентифікаційний номер та фіксується час та дата його отримання, а також рішення, прийняті в результаті його розгляду або наступного розслідування, включаючи обставини на підставі яких були прийняті такі рішення.

5.1.3. Повідомлення про порушення та реєстр отриманих повідомлень є конфіденційними та мають обмежений доступ. Менеджер з протидії шахрайству зобов’язаний вживати відповідні організаційні та технічні заходи з цією метою. З усіх питань, пов'язаних з шахрайськими діями Менеджер з протидії шахрайству підзвітний Голові Правління та аудиторському комітету Наглядової Ради та періодично надає їм інформацію про кількість отриманих повідомлень, результати ініційованих службових перевірок та вжитих заходах.

5.1.4. Начальник управління внутрішнього аудиту має право перевірити стан виконання цього Положення та отримати необхідну для цього інформацію, у тому числі від Менеджера з протидії шахрайству. При цьому від повинен забезпечити додержання конфіденційності щодо такої інформації.