Політика про захист осіб, які здійснюють службові викриття

Версії

Номер	Версія	Дата публікації
1	Випуск	31.07.2024.

Відповідальний за предмет	Інспектор(и)	Затверджувач(і)
dr. Мате Смелка (Máté Smelka) Міжнародний Спеціаліст з комплаєнсу	Крістоф Палауш (Christoph Palausch) Генеральний директор (виконавчий директор)	Професор д-р Роберт Грунінг (Robert Gröning) Генеральний директор (фінансовий директор)

Відповідні рекомендації	
Посада	Ідентифікаційний номер
Процедурна директива CPO	
Кодекс поведінки	

Огляд

I. Визначення

- **Політика** відноситься до цієї Політики про захист осіб, які здійснюють службові викриття.

- **OBO-Group:** Список компаній, що входять до групи OBO, можна знайти тут. Ця Політика не поширюється на шведську компанію OBO BETTERMANN AB.

- **Порушення** - це дії або бездіяльність, які порушують цінності або правила, викладені в Кодексі поведінки OBO-Group, а також дії або бездіяльність, які вважаються порушеннями відповідно до чинного законодавства відповідної країни.

- **Інформація про порушення** - це обґрунтовані підозри або інформація про фактичні або можливі порушення, які вже були вчинені або з високою ймовірністю будуть вчинені в межах OBO-Group або у зв'язку з діяльністю OBO-Group, а також спроби приховати такі порушення.

- **Обробка даних та інформації** - це дії і заходи, спрямовані на збір, зберігання, зміну, доповнення, використання, поширення, знеособлення, блокування і видалення даних.

- **Звіти** - це усні або письмові повідомлення інформації про порушення внутрішнім або зовнішнім органам звітності (компетентним органам відповідної країни).

- **Особа, що повідомляє, або інформатор** - це фізична особа, яка повідомляє або публічно розкриває інформацію про порушення компетентним органам, переліченим у Додатку 1 до цієї Політики (далі - "Компетентні органи"), або зовнішнім звітним органам.

- **Передбачуване порушення** - це підозра особи, яка повідомляє про порушення в організації, в якій він працює або працював раніше, або в іншій організації, якщо він вступив в контакт з цією організацією за родом своєї діяльності, в тій мірі, в якій ця підозра заснована на обґрунтованих підставах, що випливають із знань, отриманих співробітником в ході роботи від свого роботодавця або на основі знань, отриманих працівником в ході його роботи на іншому підприємстві або в організації.

- **Внутрішня звітність** - це усне або письмове доведення інформації про порушення всередині OBO-Group до компетентних органів.

- **Зовнішня звітність** - це усна або письмова передача інформації про порушення компетентним органам відповідних країн.

- **Розкриття** інформації означає доведення інформації про порушення до відома громадськості.

- **Відплата** - це будь-яка пряма або непряма дія або бездіяльність, яка відбувається в контексті, пов'язаному з роботою, викликана внутрішньою або зовнішньою звітністю або публічним розкриттям інформації і яка заподіює або може заподіяти невиправдану шкоду особі, яка повідомила (наприклад, відсторонення від роботи, звільнення тощо).

- **Наступні дії** - це дії, що вживаються внутрішнім або зовнішнім відділом звітності для перевірки достовірності та точності повідомлення, вжиття подальших заходів у зв'язку з повідомленим порушенням, відновлення правового статусу або закриття справи.

- **"Співробітник(и)"** відноситься до всіх співробітників, посадових осіб, директорів, менеджерів, акціонерів, невиконавчих членів, тимчасового персоналу, волонтерів, оплачуваних або неоплачуваних стажерів будь-якої з компаній OBO-Group.

"Положення про гендер"

З міркувань зручності читання використовується загальна форма чоловічого роду. Слід зазначити, що виключне використання форми чоловічого роду слід розуміти незалежно від статі. Це жодним чином не означає дискримінації за ознакою статі або порушення принципу рівності.

II. Сфера застосування

1. Сфера застосування матеріалу

OBO-Group прагне вести свою діяльність відповідно до найвищих етичних та правових стандартів. З цієї причини будь-яке порушення Кодексу поведінки OBO буде розглядатися з усією серйозністю.

Наступні правила покликані допомогти співробітникам, керівництву, діловим партнерам, клієнтам, постачальникам тощо OBO-Group, а також всім потенційно залученим особам (всім фізичним особам) у виявленні, інформуванні та усуненні можливих порушень в рамках OBO-Group і забезпечити безпечний канал для інформування без побоювань відплати, з метою зміцнення комплаєнсу та інформаційної культури в OBO-Group.

Про незаконну, аморальну або протиправну поведінку, а також про поведінку, яка порушує Кодекс поведінки OBO і яку працівник або зацікавлена особа не можуть зупинити самостійно, слід повідомляти контактній особі, призначеній OBO-Group. Однак система захисту осіб, які здійснюють службові викриття, не призначена для використання з метою подання скарг або засудження інших працівників загалом.

Факти/інформація/документи, незалежно від їх форми або носія, розголошення яких заборонено, оскільки на них поширюються положення про національну безпеку, захист секретної інформації, захист юридичних і медичних професійних привілеїв, таємницю судових засідань і кримінально-процесуальні норми, виключені зі сфери дії цієї Політики.

2. Сфера охоплення персоналу (цільова група)

Ця Політика поширюється на всі компанії OBO-Group і на всіх осіб, зазначених у розділах II.1 і III. 4. Ця Політика не поширюється на шведську компанію OBO BETTERMANN AB.

3. Термін дії

Ця Політика діє протягом необмеженого періоду часу з дати її опублікування до її скасування.

4. Територіальне охоплення

Ця Політика застосовується до всіх країн, де розташована компанія OBO-Group. Ця Політика не поширюється на шведську компанію OBO BETTERMANN AB.

5. Ієрархія

У тій мірі, в якій в застосовних національних правових системах існують більш суворі правила, законодавчі положення, колізійні норми тощо для окремих областей, що охоплюються цією Політикою, такі правила мають переважну силу над положеннями цієї Політики (наприклад, кримінальні злочини, дрібні правопорушення і т. д.).

III. Система захисту осіб, які здійснюють службові викриття

1. Захист осіб, які здійснюють службові викриття

(1) OBO-Group закликає всіх фізичних осіб повідомляти про порушення Кодексу поведінки через систему захисту осіб, які здійснюють службові викриття OBO-Group, якщо місцеве законодавство дозволяє таке повідомлення.

(2) Ця політика нікого не зобов'язує подавати звіти. Однак у тій мірі, в якій існують юридичні, договірні чи інші обов'язки щодо подання звітів, пропозиція 1 не зачіпає їх.

(3) Система захисту осіб, які здійснюють службові викриття служить для отримання та обробки повідомлень, а також для захисту осіб, зазначених у пункті 1, а також осіб, згаданих у розділі III. 4 "Захист інформаторів" нижче, від переслідувань, пов'язаних з повідомленнями. Однак система захисту осіб, які здійснюють службові викриття, недоступна для подання скарг загального характеру або, зокрема, для проведення загальних розслідувань. У цьому випадку, будь ласка, зверніться в нашу службу підтримки клієнтів:

Контактні дані

У Німеччині скарги відповідно до Закону про зобов'язання щодо проведення корпоративної перевірки з метою запобігання порушенням прав людини в ланцюгах поставок Німеччини (LKSG) слід подавати через контактну особу, зазначену в Додатку 1.

(4) Повідомлення слід подавати лише в тому випадку, якщо особа, яка повідомляє інформацію, діє добросовісно щодо того, що повідомлена інформація відповідає дійсності, і вона має обґрунтовані підстави вважати, що повідомлена інформація відповідає дійсності. Інформатор діє недобросовісно, якщо він знає, що повідомлена інформація не відповідає дійсності. У разі виникнення сумнівів інформація повинна бути представлена не у вигляді

фактів, а у вигляді припущень, оцінок або тверджень інших осіб. Санкції, передбачені трудовим законодавством, також не застосовуються у разі подання добросовісних звітів.

(5) Слід зазначити, що інформатори, які всупереч своєму здоровому глузду повідомляють недостовірну інформацію про інших осіб, можуть бути притягнуті до відповідальності або оштрафовані відповідно до національного законодавства.

2. Звіти

(1) Інформатори можуть направляти повідомлення в одне з компетентних відомств, використовуючи контактні дані, зазначені в Додатку 1. Надання інформації про порушення не прив'язане до будь-якої конкретної форми або мови. Інформація про порушення може бути представлена інформатором рідною мовою країни походження; компетентне відомство повинно забезпечити переклад і спілкування рідною мовою інформатора. Зокрема, звіти можуть бути подані особисто, по телефону, у письмовій або текстовій формі (наприклад, листом або електронною поштою). З метою спрощення процедури ми рекомендуємо відправляти заявки по електронній пошті. Щоб забезпечити конфіденційну обробку поштових повідомлень, ми просимо використовувати адресний суфікс "Конфіденційні повідомлення - OBO". Національне законодавство може встановлювати особливі формальні вимоги до звітності, які можуть виходити за рамки тих, які викладені в цій Політиці.

(2) Компетентні органи, зрозуміло, нададуть всім фізичним особам можливість попередньо проконсультуватися, перш ніж складати звіт. Використання консультацій не тягне за собою зобов'язання складати звіт, і компетентні відомства зобов'язані ставитися до інформації, наданої в ході консультацій, так само конфіденційно, як і до звітів.

(3) На додаток до відповідальних компетентних органів, перелічених у Додатку 1, інформатор має можливість зв'язатися із зовнішніми органами, що надають інформацію, відповідно до законодавчих положень відповідної країни, як зазначено у Додатку 3. Однак OBO-Group рекомендує спочатку звернутися до власного відділу внутрішньої звітності (компетентних органів). Інформатор повинен бути проінформований про те, що деякі місцеві закони можуть ставити захист інформатора в залежність від того, чи звернеться він спочатку до компетентних органів.

(4) Звіт також може бути складений анонімно. Однак, як правило, інформатору рекомендується розкрити свою особу, а не надсилати анонімне повідомлення. Причина в тому, що набагато важче простежити за надходженням повідомлення та провести ретельне та всебічне розслідування, якщо неможливо або важко зв'язатися з джерелом для отримання додаткової інформації. Якщо інформатор представить себе, можливо, буде легше захистити його від відплати.

(5) Компетентний орган повинен підтвердити отримання повідомлення інформатору не пізніше, ніж протягом 2 робочих днів. Після такого підтвердження компетентний орган повинен оцінити, чи підпадає заявлене порушення під дію цієї політики, і проінформувати інформатора протягом 7 днів з моменту отримання повідомлення (або протягом 3 днів з моменту прийняття відповідного рішення) про те, як класифікується повідомлення і чи буде воно розслідувано компетентним органом або переданий в компетентний департамент або орган влади.

(6) У разі, якщо національне законодавство вимагає, щоб подальші дії здійснювалися організаційним підрозділом або особою в організаційній структурі компанії, компетентне відомство, зазначене в Додатку 1, передасть це питання такому внутрішньому підрозділу або особі у відповідній компанії для проведення подальших дій. У вищезгаданому випадку такий внутрішній організаційний підрозділ або особа у відповідній компанії буде вважатися компетентним підрозділом за змістом цієї Політики в рамках здійснення подальших дій.

(7) Компетентне відомство повинно (якщо це можливо і допустимо) підтримувати контакт із інформатором, перевіряти достовірність отриманого повідомлення, при необхідності запитувати у нього додаткову інформацію і робити відповідні подальші дії.

(8) Компетентне відомство зобов'язане надати відповідь інформатору в письмовій формі протягом 30 днів з моменту підтвердження отримання повідомлення. Компетентне відомство може, проінформувавши інформатора, продовжити термін надання зворотного зв'язку на 30 днів, якщо це виправдано обставинами розслідування. Незважаючи на вищевикладене, компетентне відомство зобов'язане надати відповідь інформатору протягом 2 робочих днів після закінчення розслідування.

(9) Зворотній зв'язок повинен включати вказівку на будь-які заплановані подальші дії, а також на будь-які вже вжиті подальші дії та причини таких дій. Зворотній зв'язок, наданий інформатору, не повинен перешкоджати проведенню внутрішніх розслідувань і не буде обмежувати права осіб, які є предметом або названі у звіті.

(10) OBO-Group надає компетентному відомству повноваження, необхідні для виконання його завдань, зокрема для розгляду повідомлень, отримання інформації та здійснення подальших дій. Компетентному відомству повинні бути надані ресурси, необхідні для виконання його завдань. Компетентне відомство повинно бути незалежним при виконанні своїх завдань і може також здійснювати іншу діяльність в рамках OBO-Group за умови, що це не суперечить завданням відповідно до цієї Політики і не ставить під загрозу виконання цих завдань.

(11) Інформатори завжди зберігають за собою право не обмовлювати себе при складанні заяви.

(12) Під час розслідування конфіденційність буде дотримана відповідно до вимог ретельного розслідування та потреб OBO-Group.

3. Документування звітів

(1) Компетентне відомство має документувати всі звіти, що надходять, у постійно доступній формі відповідно до зобов'язання про конфіденційність та положень відповідного національного законодавства.

(2) У разі повідомлень по телефону, повідомлень за допомогою іншої форми голосового зв'язку або повідомлень в контексті наради повна і точна розшифровка (дослівний запис) розмови може бути зроблена тільки за згодою особи, яка повідомляє про порушення. За відсутності такої згоди компетентне відомство документує звіт у вигляді короткого викладу його змісту (протокол про зміст). Копія документа, що містить звіт, зберігається у інформатора. Компетентне відомство не повинно вести аудіозапис звітів.

(3) Інформатору повинна бути надана можливість ознайомитися і, при необхідності, внести виправлення в стенограму або протокол і підтвердити підписом або в електронній формі.

(4) Компетентний орган повинен документально підтвердити в кожному випадку, незалежно від того, чи вирішив інформатор зберегти анонімність і чи потрібна його згода відповідно до чинного законодавства про захист даних, що інформатор дав явну згоду на обробку своїх персональних даних відповідно до Додатка 2.

(5) Компетентне відомство також повинно дотримуватися будь-яких додаткових вимог до оформлення звітів, викладених у чинному законодавстві відповідної країни.

4. Захист інформаторів

(1) OBO-Group зобов'язана зберігати в таємниці особистість наступних осіб:

- інформатор і його прихильники (наприклад, свідки, близькі родичі або колеги, які надають інформацію інформатору, або які можуть зазнати переслідувань в професійному контексті, але не виступають в якості інформаторів, посередників, тобто фізичних осіб, які допомагають інформатору під час процесу подання та чия допомога має бути конфіденційною, у контексті захисту інформаторів, що далі разом іменується як: інформатор), якщо повідомлена інформація стосується порушень, які підпадають під дію Політики, або інформатор мав обґрунтовані підстави вважати, що це було так на момент повідомлення;
- особи, які є предметом звіту;
- інші особи, згадані у звіті; та
- юридичні особи, що належать інформаторам, або на які вони працюють, або з якими вони пов'язані в професійному контексті.

(2) За винятком випадків, коли це необхідно для дотримання юридичних зобов'язань, що діють у відповідній країні, включаючи ті, що випливають із законодавства ЄС, або з явної та вільної згоди осіб, згаданих у розділі 1, особа осіб, згаданих у розділі 1, або будь-яка інформація, з якої можна прямо чи опосередковано встановити їх особу, може бути розкрита лише особам, відповідальним за компетентний офіс, або особам, які здійснюють подальшу діяльність, і особам, які допомагають їм під час виконання цих завдань і лише в обсязі, необхідному для виконання цих завдань.

(3) Коли особа осіб, згаданих у розділі 1, і будь-яка інформація, з якої ця особа може бути прямо або опосередковано встановлена, розкриваються відповідно до конкретного законодавства в контексті розслідувань, що проводяться національними органами влади, або судових розглядів, зацікавлені особи будуть проінформовані про це заздалегідь, за винятком випадків, коли така інформація може поставити під загрозу розслідування або відповідні судові розгляди.

(4) Вимога про конфіденційність особистих даних має застосовуватися незалежно від того, чи несе компетентне відомство відповідальність за звіт, що надходить.

(5) Особи, які повідомляють про порушення, користуються захистом відповідно до цієї Політики тільки в тому випадку, якщо вони можуть обґрунтовано вважати, ґрунтуючись на фактичних обставинах та інформації, що доступна їм на момент подання повідомлення, інформація є достовірною і підпадає під дію цієї Політики. В іншому випадку (особливо якщо інформатор свідомо надає неправдиву інформацію) особа інформатора не захищена цією Політикою, якщо інше не передбачено чинним національним законодавством.

(6) Компетентний орган повинен відхилити завідомо неправдиву інформацію, поінформувавши інформатора про те, що така інформація може призвести до притягнення його до відповідальності за заподіяну шкоду або, залежно від положень чинного національного законодавства, може призвести до судового або адміністративного переслідування.

(7) Захист інформаторів вимагає, щоб:

- інформатор діяв сумлінно; і
- інформація, що стосується порушення в рамках цієї Політики, або особа, яка повідомила інформацію, мала обґрунтовані підстави вважати, що це було так на момент подання повідомлення; і
- захист інформатора не виключається законодавчими положеннями відповідної країни.

(8) Інформатор не може бути притягнутий до юридичної відповідальності за отримання або доступ до повідомленої ним інформації, за винятком випадків, коли отримання або доступ до інформації самі по собі є окремим кримінальним або адміністративним правопорушенням відповідно до норм чинного національного законодавства.

(9) Переслідування особи, яка повідомила про порушення, яка мала обґрунтовані підстави вважати, що інформація про порушення, про яку повідомлялося, була достовірною на момент подання заяви та підпадала під дію цієї Політики, інших осіб, згаданих у розділі 1, та роботодавця заборонено. Це також стосується загрози та спроби відплати.

(10) Якщо в контексті провадження у компетентних судах або органах влади інформатор продемонструє, що йому завдано будь-якої шкоди у зв'язку з його професійною діяльністю, і що він подав заяву відповідно до цієї Політики, така шкода буде розглядатися як відплата за подання такої заяви. У цьому випадку особа (фізична чи юридична), яка помстилася інформатору, повинна довести, що заподіяння шкоди базувалося на достатньо обґрунтованих причинах або що воно не базувалося на звіті.

(11) У разі порушення заборони на відплату відповідна особа має право вимагати компенсації за заподіяну шкоду відповідно до положень чинного національного законодавства.

(12) Якщо інформатор, проте, став жертвою відплати, це не є підставою для відмови в прийомі на роботу, у зв'язку з професійним навчанням або будь-якими іншими контрактними відносинами або в просуванні по службі.

(13) Додаткові санкції за порушення положень про захист інформаторів можуть бути передбачені законами відповідної країни про захист інформаторів.

IV. Захист даних

1. Обробка даних

(1) OBO-Group виконує свої зобов'язання відповідно до чинних законів "Про захист даних", включаючи Регламент (ЄС) 2016/679 (GDPR) і національні закони, що регулюють його застосування, і обробляє всю інформацію про порушення, незалежно від її достовірності, з особливою конфіденційністю і відповідно до чинних законодавчих положень про захист даних. У більш загальному плані, будь-яка обробка персональних даних, включаючи збір, обмін, передачу або зберігання персональних даних в рамках збору та обробки звітів і їх розслідування, буде здійснюватися відповідно до чинних законів "Про захист даних", як більш докладно описано в Додатку 2 "Повідомлення про захист даних" з внесеними в нього поправками.

(2) На додаток до каталогу обробки, який повинен правильно зберігатися і постійно оновлюватися, особи, які мають доступ до інформації та пов'язаних з нею даних, а також їх права щодо обробки, повинні бути зафіксовані в письмовій формі. Співробітники OBO-Group, які беруть участь в обробці інформації, зобов'язані ставитися до персональних даних, про які їм стає відомо у зв'язку зі звітами, як до конфіденційних, відповідно до Додатка 2 "Повідомлення про захист даних" до цієї Політики.

(3) Якщо Політика конфіденційності буде опублікована у відповідній країні відповідно до місцевого законодавства, вона автоматично стане частиною цієї Політики. У разі суперечності між політикою конфіденційності відповідно до місцевого законодавства та повідомленням про захист даних, наведеним у Додатку 2, переважну силу має Політика конфіденційності відповідно до місцевого законодавства.

2. Інформаційна безпека та безпека даних

(1) IT-рішення для отримання та обробки інформації про порушення повинні бути перевірені та схвалені омбудсменом (DR. WEHBERG UND PARTNER mbB) і, за наявності, спеціалістом із захисту даних компанії OBO-Group перед їх використанням.

(2) OBO-Group виконує свої зобов'язання щодо забезпечення безпеки обробки даних за допомогою системи IT-безпеки відповідно до статті 32 GDPR.

3. Концепція видалення

(1) В принципі, персональні дані повинні зберігатися до тих пір, поки це необхідно і пропорційно для розслідування повідомленого інциденту недотримання вимог. Після завершення всіх робіт, пов'язаних зі звітом про відповідність, компетентний орган видалить персональні дані, за винятком даних, які необхідно зберегти і обробити для здійснення і захисту прав OBO-Group.

(2) Дата видалення персональних даних, що зберігаються та обробляються OBO-Group для здійснення та захисту своїх прав, визначається закінченням максимальних строків давності щодо адміністративних та кримінальних правопорушень або для пред'явлення цивільних позовів відповідно до чинного місцевого законодавства.

(3) Дані, що стосуються повідомлення, яке не призвело або не могло призвести до дисциплінарного або судового розгляду, повинні бути знищені відразу після завершення розслідування.

(4) Вищевказане не завдає шкоди конкретним термінам зберігання даних, встановленим у чинному національному законодавстві відповідної країни, згаданому в Додатку 3, яке має переважну силу в разі суперечності з розділом 3.

V. Інші положення

1. Огляд системи захисту осіб, які здійснюють службові викриття

OBO-Group зобов'язана щорічно переглядати систему інформування і вносити в неї всі необхідні зміни.

2. Інформація по конкретній країні

Посилання на національне законодавство, список національних служб зовнішньої звітності і контактні дані національних органів із захисту даних наведені в додатку 3 до цієї Політики.

VI. Перелік додатків

Додаток 1 Компетентні органи
Додаток 2 Повідомлення про захист даних
Додаток 3 Інформація по конкретній країні