Политика оповещения о нарушениях

Версии

Номер	Версия	Дата публикации
1	Издание	31.07.2024.

Ответственный за тему	Инспектор	Утвердил
д-р. Мате Смелка Международный специалист отдела контроля за соблюдением законодательства и корпоративных стандартов	Кристоф Палауш Управляющий директор (главный операционный директор)	Профессор д-р Роберт Грёнинг Управляющий директор (главный финансовый директор)
…… (Подпись)	…… (Подпись)	…… (Подпись)

Соответствующие рекомендации	
Название	Идентификационный номер
Процедурная директива CPO	
Кодекс корпоративной этики	

Содержание

I. Определения

- **Политика** относится к настоящей Политике в отношении информаторов.

- **OBO-Group:** Список компаний, входящих в OBO Group, можно найти здесь. Настоящая политика не распространяется на шведскую компанию OBO BETTERMANN AB.

- **Нарушения** - это действия или бездействия, которые нарушают ценности или правила, изложенные в Кодексе корпоративной этики OBO-Group, а также действия или бездействия, которые считаются нарушениями в соответствии с применимым законодательством соответствующей страны.

- **Информация о нарушениях** - это обоснованные подозрения или сведения о фактических или возможных нарушениях, которые уже были совершены или с высокой вероятностью будут совершены в OBO-Group или в связи с деятельностью OBO-Group, а также попытки скрыть такие нарушения.

- **Обработка данных и информации** - это действия и меры, направленные на сбор, хранение, изменение, дополнение, использование, распространение, анонимизацию, блокировку и удаление данных.

- **Отчеты** - это устные или письменные сообщения информации о нарушениях во внутренние или внешние ведомства, принимающие отчеты (компетентные органы соответствующей страны).

- **Сообщающее лицо или информатор** - это физическое лицо, которое сообщает или публично раскрывает информацию о нарушениях компетентным ведомствам, указанным в Приложении 1 к настоящей Политике (далее именуемым "компетентные ведомства"), или внешним ведомствам, принимающим отчеты.

- **Предполагаемое нарушение** означает подозрение лица, подающего отчет, о нарушении в организации, в которой оно работает или работало, или в другой организации, если оно вступило в контакт с этой организацией в связи со своей работой, поскольку подозрение основано на разумных основаниях, вытекающих из знаний, полученных работником в ходе выполнения своих обязанностей по отношению к работодателю, или из знаний, полученных работником в ходе своей работы в другой компании или организации.

- **Внутренняя отчетность** - это устное или письменное сообщение информации о нарушениях внутри OBO-Group до компетентных органов.

- **Внешняя отчетность** - это устное или письменное сообщение информации о нарушениях компетентным органам соответствующих стран.

- **Раскрытие** информации означает доведение информации о нарушениях до сведения общественности.
- **Ответные меры** - это любое прямое или косвенное действие или бездействие, которое происходит в контексте работы, вызвано внутренней или внешней отчетностью или публичным раскрытием информации и которое причиняет или может причинить неоправданный ущерб сообщающему лицу (например, отстранение от работы, увольнение и т.д.).
- **Последующие действия -** это действия, предпринимаемые внутренним или внешним ведомством, принимающим отчеты для проверки достоверности и точности отчета, для принятия дальнейших мер в отношении заявленного нарушения, для восстановления правового статуса или для закрытия дела.

- **Сотрудник(и)** - это все работники, должностные лица, директора, руководители, акционеры, члены совета директоров, временные сотрудники, волонтеры, оплачиваемые или неоплачиваемые стажеры любой из компаний OBO-Group.

“Гендерная оговорка”

Из соображений удобства чтения используется общая форма мужского рода. Следует отметить, что исключительное использование формы мужского рода следует понимать независимо от пола. Это ни в коем случае не означает дискриминации по половому признаку или нарушения принципа равенства.

II. Сфера применения

1. Материальная сфера

OBO-Group стремится вести свою деятельность в соответствии с высочайшими этическими и правовыми стандартами. По этой причине любое нарушение Кодекса корпоративной этики OBO будет рассматриваться с максимальной серьезностью.

Следующие правила призваны помочь сотрудникам, руководству, деловым партнерам, клиентам, поставщикам и т.д. OBO-Group, а также всем потенциально затронутым лицам (всем физическим лицам) в выявлении, информировании и устранении возможных нарушений в OBO-Group и обеспечить безопасный канал для информирования без опасений ответных мер, с целью укрепления культуры соблюдения правовых и этических норм и информационной культуры в OBO-Group.

О незаконном, аморальном или противоправном поведении, а также о поведении, которое нарушает Кодекс корпоративной этики OBO и которое сотрудник или заинтересованное лицо не могут остановить самостоятельно, следует сообщать контактному лицу, назначенному OBO-Group. Однако система оповещения о нарушениях не предназначена для использования с целью подачи жалоб или осуждения других сотрудников в целом.

Факты / информация / документы, независимо от их формы или носителя, раскрытие которых запрещено, поскольку они касаются национальной безопасности, защиты секретной информации, защиты юридической и врачебной профессиональной тайны, тайны судебных заседаний и уголовно-процессуальных норм, исключены из сферы применения настоящей Политики.

2. Персонал (целевая группа)

Настоящая Политика распространяется на все компании OBO-Group и на всех лиц, указанных в разделах II.1 и III.4. Настоящая Политика не распространяется на шведскую компанию OBO BETTERMANN AB.

3. Временные рамки

Настоящая Политика применяется на неограниченный срок с момента ее публикации до ее отмены.

4. Территориальные рамки

Настоящая Политика применяется ко всем странам, где расположена компания OBO-Group. Настоящая Политика не распространяется на шведскую компанию OBO BETTERMANN AB.

5. Иерархия

В той степени, в которой в применимых национальных правовых системах для отдельных областей, охватываемых настоящей Политикой, существуют более строгие правила, законодательные положения, коллизионные нормы и т.д. такие правила имеют преимущественную силу перед положениями настоящей Политики (например, уголовные преступления, мелкие правонарушения и т.д.).

III. Система оповещения о нарушениях

1. Информатор

(1) OBO-Group призывает всех физических лиц подавать отчеты через систему оповещения о нарушениях OBO-Group, если им станет известно о нарушении Кодекса корпоративной этики OBO-Group и если местное законодательство разрешает такие отчеты.

(2) Настоящая Политика не обязывает никого подавать отчеты. Однако в той степени, в которой существуют юридические, договорные или другие обязанности или обязательства по подаче отчетов, они не затрагиваются пунктом 1.

(3) Система оповещения о нарушениях служит для приема и обработки отчетов и для защиты лиц, указанных в пункте 1, а также лиц, упомянутых в разделе III. 4 “Защита информаторов” ниже, от ответных мер, связанных с отчетами. Однако система оповещения о нарушениях недоступна для подачи жалоб общего характера или, в частности, для проведения общих расследований. В этом случае, пожалуйста, обратитесь в нашу службу поддержки клиентов:

Контакт

В Германии жалобы в соответствии с немецким законом об обязательствах по проведению корпоративной проверки в целях предотвращения нарушений прав человека в цепочках поставок (LKSG) следует подавать через контактное лицо, указанное в Приложении 1.

(4) Отчеты должны подаваться только в том случае, если информатор действует добросовестно, полагая, что сообщенная информация соответствует действительности, и у информатора есть разумные основания полагать, что сообщенная информация является правдой. Информатор действует недобросовестно, если он знает, что сообщенная информация не соответствует действительности. В случае возникновения сомнений информация должна быть представлена не в виде фактов, а в виде предположений, оценок или утверждений других лиц. Санкции, предусмотренные трудовым законодательством, также не применяются в случае представления добросовестных отчетов.

(5) Следует отметить, что информаторы, которые вопреки своему здравому смыслу сообщают недостоверную информацию о других лицах, могут быть привлечены к уголовной ответственности или оштрафованы в соответствии с национальным законодательством.

2. Отчеты

(1) Информаторы могут подавать отчеты в один из компетентных ведомств, используя контактные данные, указанные в Приложении 1. Предоставление информации о нарушениях не привязано к какой-либо конкретной форме или языку. Информация о нарушениях может быть представлена информатором на родном языке страны происхождения; компетентное ведомство должно обеспечить перевод и общение на родном языке информатора. В частности, отчеты могут быть представлены лично, по телефону, в письменной или текстовой форме (например, письмом или по электронной почте). В целях упрощения процедуры мы рекомендуем отправлять отчеты по электронной почте. Чтобы обеспечить конфиденциальную обработку почтовых уведомлений, мы просим использовать адресное дополнение «КОНФИДЕНЦИАЛЬНО - Уведомления ОВО». Национальное законодательство может устанавливать особые формальные требования к отчетности, которые могут выходить за рамки тех, которые изложены в настоящей Политике.

(2) Компетентные ведомства, разумеется, предоставят всем физическим лицам возможность предварительной консультации перед подачей отчета. Использование консультаций не влечет за собой обязательства составлять отчет, и компетентные ведомства обязаны относиться к информации, предоставленной в ходе консультаций, так же конфиденциально, как и к отчетам.

(3) В дополнение к ответственным компетентным ведомствам, перечисленным в Приложении 1, у информатора есть возможность связаться с внешними ведомствами, принимающими отчеты, в соответствии с законодательными положениями соответствующей страны, как указано в Приложении 3. Однако OBO-Group рекомендует сначала обратиться в свое собственное внутреннее ведомство, принимающее отчеты (компетентные ведомства). Информатор должен быть проинформирован о том, что в соответствии с некоторыми местными законами защита информатора может зависеть от того, обратится ли он сначала в компетентные ведомства.

(4) Отчет также может быть подан анонимно. Однако, как правило, информатору рекомендуется раскрыть свою личность, а не подавать анонимный отчет. Причина в том, что гораздо труднее отследить отчет и провести тщательное и всестороннее расследование, если невозможно или затруднительно связаться с источником для получения дополнительной информации. Если информатор идентифицирует себя, возможно, его будет легче защитить от ответных мер.

(5) Компетентное ведомство должно подтвердить получение отчета информатору не позднее, чем в течение 2 рабочих дней. После такого подтверждения компетентное ведомство должно оценить, относится ли заявленное нарушение к материальной сфере настоящей Политики, и уведомить информатора в течение 7 дней с момента получения отчета (или в течение 3 дней с момента принятия соответствующего решения) о классификации отчета и о том, будет ли он расследоваться компетентным ведомством или передан в компетентный отдел или орган власти.

(6) В случае, если национальное законодательство требует, чтобы последующие действия осуществлялись организационным подразделением или лицом в организационной структуре компании, компетентное ведомство, указанное в Приложении 1, передаст этот вопрос такому внутреннему подразделению или лицу в соответствующей компании для проведения последующих действий. В вышеупомянутом случае такое внутреннее организационное подразделение или лицо в соответствующей компании будет считаться компетентным ведомством в значении настоящей Политики в рамках осуществления последующих действий.

(7) Компетентное ведомство должно (если это возможно и допустимо) поддерживать контакт с информатором, проверять достоверность полученного отчета, при необходимости запрашивать у него дополнительную информацию и предпринимать соответствующие последующие действия.

(8) Компетентное ведомство обязано предоставить обратную связь информатору в письменной форме в течение 30 дней с момента подтверждения получения отчета. Компетентное ведомство может, уведомив об этом информатора, продлить срок предоставления обратной связи на 30 дней, если это оправдано обстоятельствами расследования. Несмотря на вышеизложенное, компетентное ведомство обязано предоставить обратную связь информатору в течение 2 рабочих дней после окончания расследования.

(9) Обратная связь должна содержать указание на любые планируемые последующие действия, а также на любые уже предпринятые последующие действия и причины таких действий. Обратная связь, предоставленная информатору, не должна препятствовать проведению внутренних расследований и не будет ущемлять права лиц, ставших предметом отчета или названных в нем.

(10) OBO-Group предоставляет компетентному ведомству полномочия, необходимые для выполнения его задач, в частности для рассмотрения уведомлений, получения информации и осуществления последующих действий. Компетентное ведомство должно быть обеспечено ресурсами, необходимыми для выполнения своих задач. Компетентное ведомство должно быть независимым при выполнении своих задач и может также осуществлять другую деятельность в рамках OBO-Group при условии, что это не противоречит задачам в соответствии с настоящей Политикой и не ставит под угрозу выполнение этих задач.

(11) Информаторы всегда сохраняют за собой право не свидетельствовать против себя при составлении отчета.

(12) В ходе расследования конфиденциальность будет поддерживаться в максимально возможной степени, согласуясь с проведением тщательного расследования и потребностями OBO-Group.

3. Документирование отчетов

(1) Компетентное ведомство должно документировать все поступающие отчеты в постоянно доступной форме в соответствии с обязательством о конфиденциальности и положениями соответствующего национального законодательства.

(2) В случае предоставления отчета по телефону или посредством другой формы голосовой связи или отчетов в контексте встречи, полная и точная расшифровка (дословная запись) разговора может быть сделана только с согласия информатора. При отсутствии такого согласия компетентное ведомство документирует отчет в виде краткого изложения его содержания (протокол содержания). Копия документа, содержащего отчет, хранится у информатора. Компетентное ведомство не должно вести аудиозапись отчетов.

(3) Информатору должна быть предоставлена возможность ознакомиться и, при необходимости, внести исправления в расшифровку или протокол и подтвердить это подписью или в электронной форме.

(4) Компетентное ведомство в каждом случае документирует, решил ли информатор сохранить анонимность, и, если требуется согласие информатора в соответствии с применимым законодательством о защите данных, что информатор дал явное согласие на обработку своих персональных данных в соответствии с Приложением 2.

(5) Компетентное ведомство также должно соблюдать любые дополнительные требования к оформлению отчетов, изложенные в применимом законодательстве соответствующей страны.

4. Защита информаторов

(1) OBO-Group обязана сохранять в тайне личность следующих лиц:

- информатора и его сторонников (например, свидетелей, близких родственников или коллег, которые предоставляют информацию информатору, или которые могут подвергнуться наказанию в профессиональном контексте, но не выступают в качестве информаторов, посредников, т.е. физических лиц, которые помогают информатору в процессе подачи отчета о нарушениях и чья помощь должна быть конфиденциальной в контексте защиты информатора, далее совместно именуемых: информатор), поскольку представленная информация касается нарушений, подпадающим под действие Политики, или у информатора были разумные основания полагать, что это имело место на момент представления отчета,
- лиц, являющиеся предметом отчета,
- других лиц, упомянутых в отчете, и
- юридических лиц, относящихся к информаторам, или на которые они работают, или с которыми они связаны в профессиональном контексте.

(2) За исключением целей соблюдения правовых обязательств, действующих в соответствующей стране, в том числе вытекающих из законодательства ЕС, или с явного и свободного согласия лиц, упомянутых в разделе 1, личность лиц, упомянутых в разделе 1, или любая информация, из которой прямо или косвенно может быть установлена их личность, может быть раскрыта только лицам, ответственным за компетентное ведомство или лицам, осуществляющим последующую деятельность, а также лицам, помогающим им в выполнении этих задач, и только в объеме, необходимом для выполнения этих задач.

(3) Когда личность лиц, упомянутых в разделе 1, и любая информация, из которой эта личность может быть прямо или косвенно установлена, раскрываются в соответствии с конкретным законодательством в контексте расследований, проводимых национальными органами власти, или судебных разбирательств, соответствующие лица будут проинформированы об этом заранее, за исключением случаев, когда такая

информация может поставить под угрозу соответствующие расследования или судебные разбирательства.

(4) Требование о конфиденциальности личных данных применяется независимо от того, является ли компетентное ведомство ответственным за поступивший отчет.

(5) Информаторы пользуются защитой в соответствии с настоящей Политикой только в том случае, если они могут обоснованно полагать, основываясь на фактических обстоятельствах и информации, доступной им на момент представления отчета, что их информация является достоверной и подпадает под действие настоящей Политики. В противном случае (особенно если информатор сознательно предоставляет ложную информацию) личность информатора не защищается настоящей Политикой, если иное не предусмотрено применимым национальным законодательством.

(6) Компетентное ведомство должно отклонить заведомо ложную информацию, уведомив информатора о том, что такая информация может повлечь за собой ответственность информатора за причиненный ущерб или, в зависимости от положений применимой национальной правовой системы, может подвергнуть информатора риску судебного или административного преследования.

(7) Защита информаторов требует, чтобы
- информатор действовал добросовестно, и
- информация касалась нарушения, подпадающего под действие настоящей Политики, или информатор имел разумные основания полагать, что это имело место на момент представления отчета, и
- защита информатора не исключается правовыми положениями соответствующей страны.

(8) Информатор не может быть привлечен к юридической ответственности за получение или доступ к сообщенной им информации, за исключением случаев, когда получение или доступ к информации сами по себе являются отдельным уголовным или административным правонарушением в соответствии с нормами применимого национального законодательства.

(9) Запрещены ответные действия в отношении информатора, который имел разумные основания полагать, что сообщенная информация о нарушениях была правдивой на момент сообщения и подпадала под действие настоящей Политики, а также в отношении других лиц, указанных в пункте 1, и Работодателя. Это также относится к угрозам и попыткам возмездия.

(10) Если в контексте разбирательства в компетентных судах или органах власти информатор продемонстрирует, что ему причинен какой-либо вред в связи с его профессиональной деятельностью, и что он представил отчет в соответствии с настоящей Политикой, такой вред будет рассматриваться как возмездие за подачу такого отчета. В этом случае лицо (физическое или юридическое), принявшее ответные меры в отношении информатора,

должно доказать, что причинение вреда было основано на достаточно обоснованных причинах или что оно не было основано на отчете.

(11) В случае нарушения запрета на возмездие соответствующее лицо имеет право требовать компенсации за причиненный ущерб в соответствии с положениями применимой национальной правовой системы.

(12) Если информатор все же стал жертвой возмездия, это не будет являться основанием для требования о трудоустройстве, профессиональной подготовке или любых других договорных отношениях или карьерного продвижения.

(13) Дополнительные санкции за нарушение положений о защите информаторов могут быть предусмотрены законами соответствующей страны о защите информаторов.

IV. Защита данных

1. Обработка данных

(1) OBO-Group выполняет свои обязательства в соответствии с применимыми законами о защите данных, включая Регламент (ЕС) 2016/679 (Генеральный регламент о защите персональных данных) и национальные законы, регулирующие его применение, и обрабатывает всю информацию о нарушениях, независимо от ее достоверности, с особой конфиденциальностью и в соответствии с применимыми законодательными положениями о защите данных. В целом, любая обработка персональных данных, включая сбор, обмен, передачу или хранение персональных данных в рамках сбора и обработки отчетов и их расследования, будет осуществляться в соответствии с применимыми законами о защите данных, как более подробно описано в Приложении 2 "Уведомление о защите данных" с периодическими поправками.

(2) В дополнение к справочнику по обработке данных, который должен вестись правильно и постоянно обновляться, лица, имеющие доступ к информации и связанным с ней данным, а также их права в отношении обработки, должны быть зафиксированы в письменной форме. Сотрудники OBO-Group, участвующие в обработке информации, обязаны относиться к персональным данным, ставшим им известными в связи с отчетами, как к конфиденциальным, в соответствии с Приложением 2 "Уведомление о защите данных" к настоящей Политике.

(3) Если политика конфиденциальности опубликована в соответствующей стране согласно местному законодательству, она автоматически становится частью настоящей Политики. В случае противоречия между политикой конфиденциальности в соответствии с местным законодательством и Уведомлением о защите данных, приведенным в Приложении 2, преимущественную силу имеет политика конфиденциальности в соответствии с местным законодательством.

2. IT-безопасность и безопасность данных

(1) ИТ-решения для получения и обработки информации о нарушениях должны быть проверены и одобрены омбудсменом (DR. WEHBERG UND PARTNER mbB) и - при наличии - специалистом по защите данных компании OBO-Group перед их использованием.

(2) OBO-Group выполняет свои обязательства по обеспечению безопасности обработки данных посредством системы ИТ-безопасности в соответствии со статьей 32 Генерального регламента о защите персональных данных.

3. Концепция удаления данных

(1) По общему правилу персональные данные хранятся столько, сколько необходимо и соразмерно для расследования инцидента соответствия, о котором было сообщено. После завершения всех работ, связанных с отчетом о соответствии, компетентное ведомство удаляет персональные данные, за исключением данных, которые необходимо сохранить и обработать для осуществления и защиты прав OBO-Group.

(2) Дата удаления персональных данных, хранящихся и обрабатываемых OBO-Group для осуществления и защиты своих прав, определяется истечением максимальных сроков давности по административным и уголовным правонарушениям или для предъявления гражданских исков в соответствии с применимым местным законодательством.

(3) Данные, относящиеся к отчету, который не привел или не мог привести к дисциплинарному или судебному разбирательству, должны быть уничтожены сразу после завершения расследования.

(4) Вышесказанное не затрагивает конкретных сроков хранения данных, установленных применимым национальным законодательством соответствующей страны, указанным в Приложении 3, которые имеют преимущественную силу в случае разногласия с разделом 3.

V. Прочие положения

1. Обзор системы оповещения о нарушениях

OBO-Group обязана ежегодно пересматривать систему оповещения и вносить в нее все необходимые изменения.

2. Информация по конкретной стране

Ссылки на национальное законодательство, список национальных внешних органов по отчетности и контактные данные национальных органов по защите данных приведены в Приложении 3 к настоящей Политике.

VI. Перечень приложений

Приложение 1 Компетентные органы
Приложение 2 Уведомление о защите данных
Приложение 3 Информация по конкретной стране