SIEMENS

Обязательные корпоративные правила («ОКП») - Краткий обзор прав третьих лиц

Настоящий документ содержит в Разделах 3-9 все положения «Обязательных корпоративных правил (ОКП) для компаний Группы «Сименс» и других присоединяющихся компаний по защите персональных данных», которые являются обязательными по отношению к субъектам данных в силу прав сторонних бенефициаров.

1. Цель Обязательных корпоративных правил

Защита безопасности и конфиденциальности персональных данных важна для «Сименс». Поэтому «Сименс» ведет свою деятельность в соответствии с действующим законодательством о защите конфиденциальности и защите данных. ОКП являются внутренними правилами, принятыми «Сименс», то есть Siemens AG и ее компаниями-участниками, для предоставления «адекватных гарантий защиты частной жизни и основных прав и свобод физических лиц» по смыслу применимого закона о защите данных, в частности, законов о защите данных государств-членов Европейской экономической зоны («**ЕЭЗ**»).

2. Область применения Обязательных корпоративных правил

ОКП применяется к обработке всех персональных данных, относящихся к субъектам данных, компаниями-участниками, учрежденными

- за пределами ЕЭЗ, в той мере, в которой эти персональные данные были переданы от компании-участника, учрежденной в стране ЕЭЗ или учрежденной в стране с адекватным уровнем защиты данных, что было подтверждено решением Комиссии ЕС, компании-участнику, учрежденной за пределами ЕЭЗ; а также
- в стране ЕЭЗ или в стране с адекватным уровнем защиты данных, что было подтверждено решением Комиссии ЕС.

3. Основные принципы обработки персональных данных

Следующие принципы, которые вытекают из Директивы ЕС по защите данных 95/46/ЕС и Резолюции Мадрида от 5 ноября 2009 года, применяются к обработке персональных данных компаниями-участниками в рамках настоящих ОКП:

3.1. Правомерность и законность обработки данных

Обработка персональных данных должна осуществляться на законных основаниях в соответствии с соответствующими нормами законодательства и с должным учетом принципов, изложенных в настоящих ОКП.

Обработка разрешается только в том случае, если выполняется хотя бы одно из следующих условий:

- Субъект данных добровольно дал свое однозначное и действительно согласие; или
- Обработка данных предназначена для установления договорных отношений или аналогичных отношений доверия с субъектом данных; или
- Обработка необходима для защиты обоснованных интересов контролера (для целей настоящих ОКП под «**контролером**» понимается компания, которая определяет цели и средства обработки данных; зависимые филиалы, места осуществления деловых операций и обособленные подразделения являются частью контролера), и нет оснований полагать, что субъект данных имеет преимущественное законное право препятствовать обработке данных; или
- Обработка предусмотрена или разрешена национальным законодательством и нормативными актами, которые применяются к контролеру; или
- Обработка необходима для выполнения юридических обязательств, которые имеет контролер; или
- Обработка необходима в исключительных случаях для защиты жизни, здоровья или безопасности субъекта данных.

Контролер должен предоставить простые, быстрые и эффективные процедуры, позволяющие субъекту данных отозвать свое согласие в любое время.

3.2. Цель

Персональные данные обрабатываются исключительно в установленных, прямо выраженных и законных целях. Ни при каких обстоятельствах персональные данные не должны обрабатываться каким-либо образом, несовместимым с законными целями, для которых собирались персональные данные. Компании-участники обязаны придерживаться этих первоначальных целей при хранении и дальнейшей обработке или использовании данных, переданных им другой компанией-участником; цель обработки данных может быть изменена только с согласия субъекта данных или в пределах, разрешенных национальным законодательством, которому подчиняется компания-участник, передающая данные.

3.3. Прозрачность

Все компании-участники должны обрабатывать персональные данные прозрачным образом. Субъекты данных, чьи персональные данные обрабатываются компанией-участником, получают от компании-участника следующую информацию (по согласованию с передающей компанией, если применимо):

- Идентификационные данные контролера и передающей компании;
- Категории получателей или идентификационные данные получающей организации;
- Цель обработки;
- Происхождение данных (за исключением персональных данных, которые собираются непосредственно у субъекта данных);
- Право возражения против обработки персональных данных субъекта данных в рекламных целях;
- Другая информация в объеме, требуемом по соображениям права справедливости, например прав на исправление и стирание информации.

Если персональные данные не собирались непосредственно у субъекта данных, такая информация - в качестве исключения – не обязательно должна предоставляться, если такое непредоставление информации необходимо для защиты субъекта данных или прав других лиц, если субъект данных уже был проинформирован или если это потребует непропорциональных усилий.

3.4. Качество данных и экономия данных

Персональные данные должны быть фактически правильными и, при необходимости, обновляться. Соответствующие меры должны быть приняты для исправления или удаления неточных или неполных данных.

Обработка данных должна основываться на принципе экономии данных. Цель заключается в сборе, обработке и использовании только таких персональных данных, которые требуются, т. е. как можно меньшего объема персональные данных. В частности, следует использовать возможность использования анонимных или псевдонимных данных при условии, что затраты и усилия будут соразмерны с желаемой целью. Статистические оценки или исследования, основанные на анонимных или псевдоанонимизированных данных, не имеют отношения к целям защиты данных при условии, что такие данные не могут использоваться для идентификации субъекта данных.

Персональные данные, которые больше не требуются для коммерческих целей, для которых они были первоначально собраны и хранились, должны быть удалены. В случае, если применяются установленные законом сроки хранения, данные должны быть заблокированы, а не стерты.

3.5. Передача данных

Передача персональных данных от компании-участника компании, не являющейся участником (т. е. компании, не связанной обязательствами по ОКП), за пределами ЕЭЗ допускается только при соблюдении следующих условий:

- Получающая организация обеспечивает достаточный уровень защиты персональных данных по смыслу статьи 25 Директивы ЕС 95/46/ЕС о защите данных, например, путем заключения типового договора ЕС (Стандартные договорные условия относительно обработчиков данных 2010/87/ЕС или Стандартные договорные условия относительно контролеров данных 2001/497/ЕС или 2004/915/ЕС) или путем заключения других соответствующих договорных соглашений между передающей и получающей организациями;
- Передача разрешена в соответствии с исключениями, определенными в статье 26 Директивы ЕС 95/46/ЕС о защите данных;
- Если получающая организация является обработчиком персональных данных, условия, изложенные в статьях 16 и 17 Директивы ЕС о защите данных 95/46/ЕС, также должны выполняться.

3.6. Специальные категории персональных данных

Специальные категории персональных данных, то есть информация о расовом или этническом происхождении, политических взглядах, религиозных или философских убеждениях, членстве в профсоюзах, здоровье или сексуальной жизни лица, как правило не подлежат обработке.
В случае необходимости обработки специальных категорий персональных данных необходимо получить прямое согласие субъекта данных, за исключением случаев, когда:

- субъект данных не в состоянии дать свое согласие (например, в случае необходимости оказания срочной медицинской помощи), и такая обработка необходима для защиты жизненно важных интересов субъекта данных или другого лица;
- обработка необходима в связи с медицинской диагностикой, медицинскими профилактическими мероприятиями, оказанием медицинской помощи, лечением или организацией медицинских услуг, когда обработка данных осуществляется медицинским персоналом, который обязан хранить профессиональную тайну, или другим персоналом, имеющим эквивалентное обязательство по сохранению секретности;
- субъект данных уже опубликовал рассматриваемые данные;
- обработка необходима для предъявления, осуществления или защиты судебных исков в судебных разбирательствах при условии, что нет оснований полагать, что субъект данных имеет преимущественное законное право препятствовать обработке данных;
- обработка разрешена законом в соответствии с применимым национальным законодательством (например, с целью регистрации / защиты меньшинств), а также дополнительные гарантии по смыслу Директивы ЕС о защите данных 95/46/EC предоставляются в отношении обработки данных, в том числе в частности, достаточные меры безопасности для этих данных.

Перед обработкой специальных категорий персональных данных следует проконсультироваться с компетентным сотрудником компании-участника, ответственным за защиту данных (DPO).

3.7. Автоматизированные индивидуальные решения

Если персональные данные обрабатываются с целью принятия автоматизированных индивидуальных решений, законные интересы субъекта данных должны соблюдаться с помощью соответствующих мер. Решения, которые имеют негативные юридические последствия для субъекта данных или, по существу, наносят ущерб субъекту данных, не могут быть приняты исключительно на основе автоматизированной индивидуальной процедуры, предназначенной для оценки личных характеристик физического лица, то есть решения не могут основываться исключительно на использовании информационных технологий. Исключение применяется только в том случае, если решение:

- принимается в ходе заключения или исполнения договора, если поданный субъектом данных запрос о заключении или исполнении договора был выполнен, или если существуют подходящие меры для защиты его законных интересов, например, дающие ему возможность высказать свою точку зрения;
- принимается по закону, который также устанавливает меры по защите законных интересов субъекта данных.

3.8. Защита данных

Контролеры должны принимать соответствующие технические и организационные меры для обеспечения необходимой защиты данных от случайного или незаконного стирания, несанкционированного использования, изменения, потери, уничтожения, а также от несанкционированного раскрытия или несанкционированного доступа. Принимая во внимание современный уровень развития техники и стоимость реализации, такие меры должны обеспечивать уровень безопасности, соответствующий рискам, связанным с обработкой и характером защищаемых данных. Специальным категориям персональных данных должна быть предоставлена особая защита.

Предусмотренные меры безопасности относятся, в частности, к компьютерам (серверам и компьютерам на рабочем месте), сетям, линиям связи и приложениям.

Чтобы обеспечить достаточный уровень технических и организационных мер по защите данных, компания «Сименс» ввела Руководство по корпоративной информационной безопасности, имеющее обязывающую силу для всей группы «Сименс».

Конкретные меры, используемые для обеспечения надлежащей защиты персональных данных, включают в себя средства управления допуском, средства контроля доступа к системе, средства контроля доступа к данным, средства управления передачей, системы контроля входных данных, средства управления заданиями, средства контроля доступности и средства контроля сегрегации.

Все компьютеры на рабочем месте, включая мобильные устройства (например, ноутбуки), защищены паролем. Интранет «Сименс» имеет систему межсетевого экрана для защиты внутренней информации компании от несанкционированного внешнего доступа. Передача персональных данных внутри собственной сети компании обычно зашифровывается - в зависимости от характера и цели персональные данных.

3.9. Конфиденциальность обработки данных

Только персонал, уполномоченный и специально проинструктированный в отношении соблюдения требований конфиденциальности данных, может собирать, обрабатывать или использовать персональные данные. Санкционированный доступ отдельных сотрудников ограничивается в зависимости от характера и объема их конкретной области деятельности. Сотруднику запрещается использовать персональные данные для персональные целей, передавать или предоставлять персональные данные другим лицам без права доступа. Лица без права доступа в этом контексте включают, например, других сотрудников, если им не требуются персональные данные для выполнения своих специализированных задач. Обязательство по сохранению конфиденциальности остается в силе после окончания трудовых отношений с соответствующим сотрудником.

3.10. Поручение обработки данных

Если компания-участник поручает другой компании («**обработчик персональных данных**») обрабатывать персональные данные в соответствии с условиями настоящих ОКП, должны соблюдаться следующие требования:

- Обработчик персональных данных должен быть тщательно выбран контролером. Необходимо выбрать обработчика персональных данных, который может обеспечить необходимые технические и организационные меры безопасности, требующиеся для обработки данных в соответствии с правилами конфиденциальности данных;
- Контролер должен обеспечить и регулярно проверять, чтобы обработчик персональных данных полностью соблюдал согласованные технические и организационные меры безопасности;
- Выполнение порученной обработки данных должно регулироваться письменным или иным образом документированным договором, в котором права и обязанности обработчика персональных данных однозначно определены;
- Обработчик персональных данных должен быть связан договором в части обработки данных, полученных от контролера, только в рамках условий договора и в соответствии с инструкциями контролера. Обработка данных для собственных целей обработчика персональных данных или для целей третьей стороны должна быть запрещена договором;
- Контролер сохраняет ответственность за законность обработки и продолжает оставаться контактным лицом для субъекта данных.

4. Основные права субъекта данных

Субъекты данных имеют неотъемлемые права, перечисленные ниже, в отношении своих персональных данных, обрабатываемых компанией-участником в рамках настоящих ОКП.

- Субъект данных может потребовать, чтобы ему предоставили в понятной форме его обработанные персональные данные, любую имеющуюся информацию относительно их источника и цели обработки. Субъект данных также имеет право на получение информации о личности контролера, и в случае передачи персональных данных субъект данных также имеет право на получение информации о получателях или категориях получателей. Право на получение информации также включает логическую структуру операций автоматизированной обработки в той степени, в которой это затрагивает автоматизированные решения. Если предусмотрено применимым местным законодательством, субъект данных не будет иметь права на получение информации, если предоставление такой информации приведет к значительному ухудшению в достижении целей бизнеса, в том числе в том случае, если раскрытие коммерческой тайны и право на защиту коммерческой тайны перевешивают право субъекта данных на раскрытие информации. Местные нормативные акты могут ограничивать право субъекта данных на получение информации, если это право осуществляется повторно в течение короткого периода времени, если только субъект данных не может обосновать законность повторного требования предоставить информацию. Компания-участник может взимать разумную плату с субъекта данных за предоставление информации в тех случаях, когда это разрешается применимым национальным законодательством.
- Субъект данных может потребовать исправления, если его персональные данные оказались неправильными или неполными.
- Субъект данных имеет право потребовать заблокировать свои персональные данные, если невозможно установить, являются ли данные правильными или неправильными.
- Субъект данных имеет право потребовать удалить его персональные данные, если обработка данных была незаконной или стала незаконной впоследствии, или если данные перестали требоваться для целей

обработки. Обоснованные требования субъекта данных удалить данные должны выполняться в течение разумного периода времени в той степени, в которой установленные законом сроки хранения или договорные обязательства не препятствуют удалению. В случае установленных законом периодов хранения субъект данных может потребовать, чтобы его данные были заблокированы, а не удалены. То же самое применяется в том случае, если невозможно удалить данные.

- Субъект данных имеет право на **предъявление возражений** против обработки своих персональных данных в рекламных целях или для целей исследования рынка и / или опроса общественного мнения. Субъект данных должен быть проинформирован о своем праве на предъявление возражений на безвозмездной основе.
- Субъект данных также имеет **общее право на предъявление возражений** против обработки его персональные данных, если из-за особой личной ситуации субъекта данных законные права субъекта данных перевешивают законные права контролера при обработке персональных данных.

Субъект данных может заявить вышеуказанные права в письменной форме в отношении соответствующей компании-участника, компетентного сотрудника такой компании-участника, ответственного за защиту данных (DPO), или отдела по глобальной защите персональных данных (LC CO DP) Siemens AG. Ответ на обоснованный запрос субъекта данных должен быть предоставлен в разумный срок. Ответ должен быть в письменной форме (достаточно электронной почты).

5. Обязывающий характер по отношению к субъектам данных

Положения ОКП, содержащиеся в Разделах 3-9 настоящего документа, также являются обязательными для исполнения по отношению к субъектам данных в силу прав сторонних бенефициаров.

Субъекты данных могут решить подать жалобу на несоблюдение положений ОКП, содержащихся в настоящем документе, компанией-участником либо против компании-участника, либо против Siemens AG (LC CO DP).

Кроме того, субъекты данных имеют право принудительно обеспечить соблюдение прав сторонних бенефициаров компаниями-участниками подав жалобу в компетентный орган по защите данных или добиваясь получения других средств правовой защиты в компетентных судах. Субъекты данных могут потребовать компенсацию за ущерб.

Субъекты данных могут по своему усмотрению подать такую жалобу

- в юрисдикции компании-участника, которая передала данные; или
- в юрисдикции штаб-квартиры Siemens AG; или
- в компетентный орган по защите данных.

Это означает, что в случае нарушения положений ОКП компанией-участником, учрежденной за пределами ЕЭЗ, суды и органы власти на территории ЕЭЗ также обладают надлежащей юрисдикцией. Субъект данных имеет те же права в отношении компании-участника, которая взяла на себя ответственность, как если бы нарушение было совершено компанией-участником, учрежденной в стране ЕЭЗ.

Однако компетенция судов и органов власти на территории ЕЭЗ, как описано выше, не применяется, если получатель данных учрежден в стране, не входящей в ЕЭЗ, но эта страна фактически обеспечивает достаточный уровень защиты данных, что подтверждено решением Комиссии ЕС.

Для обеспечения осуществления субъектами данных юридически закрепленных прав сторонних бенефициаров также в тех странах, где предоставление прав сторонних бенефициаров ОКП может оказаться недостаточным, Siemens AG заключит в той мере, в которой это необходимо, дополнительные договорные соглашения с соответствующими компаниями-участниками. Оговорка о сторонних бенефициарах, предоставляющая необходимые права субъектам данных, включена в Декларацию о приверженности, которую подписывают компании групп, чтобы подтвердить свое принятие и выполнение ОКП. То же самое относится к Соглашению о присоединении, которое другие присоединяющиеся компании заключают с Siemens AG.

6. Процесс подачи жалобы

Субъекты данных могут подать жалобу в компетентный отдел по работе с жалобами в Siemens AG (LC CO DP, для получения контактной информации см. Раздел 10) или компетентному местному контактному лицу компании-участника по защите данных (как правило, сотруднику, ответственному за защиту данных (DPO)) в любое время на нарушение ОКП компанией-участником или обратиться с любыми вопросами. Субъекту данных должно быть предоставлено оперативное подтверждение получения жалобы соответствующим лицом или органом. Жалоба должна быть обработана в течение трех (3) месяцев с момента получения жалобы. Этот срок может быть превышен в разумных пределах в случае задержек, не относящихся к компании-участнику, например, в случае несвоевременного представления субъектом данных информации, которая является обоснованно необходимой.

Сотрудники, занимающиеся обработкой жалоб в компетентном отделе по работе с жалобами, получают соответствующий уровень независимости при осуществлении этой функции.

В отношении любого запроса компания-участник и LC CO DP обязаны сотрудничать с органами защиты данных страны и уважать их мнение.

7. Взаимная помощь и сотрудничество при взаимодействии с органами защиты данных

Siemens AG и компании-участники должны добросовестно сотрудничать и поддерживать друг друга в случае запросов и жалоб от субъектов данных в отношении несоблюдения ОКП.
Siemens AG и компании-участники также обязуются добросовестно сотрудничать с компетентными органами защиты данных в контексте реализации ОКП. Они должны отвечать на запросы, связанные с ОКП, от органов защиты данных в соответствующие сроки и соответствующим образом и должны следовать рекомендациям и решениям компетентного органа по защите данных в отношении реализации ОКП.

8. Взаимосвязь между ОКП и местными нормативными актами

Правомерность обработки персональных данных оценивается с учетом применимого местного законодательства. В тех случаях, когда применимое местное законодательство предусматривает более высокий уровень защиты персональных данных, чем настоящие ОКП, обработка данных должна соответствовать применимому законодательству. Каждая компания-участник осуществляет самостоятельную проверку (например, сотрудник, ответственный за защиту данных (DPO), или юридический отдел), существуют ли такие местные нормативные акты (например, законы о конфиденциальности данных), и обеспечивает их соблюдение. Если применимое местное законодательство предусматривает более низкий уровень защиты персональных данных, чем настоящие ОКП, применяются настоящие ОКП.

В случае, если обязательства, вытекающие из применимого местного законодательства, противоречат ОКП, компания-участник должна незамедлительно сообщить LC C DP. LC C DP фиксирует такие противоречия.

LC C DP сообщает всем компаниям-участникам, которые ранее передавали данные рассматриваемой компании-участнику, о сообщенном противоречии между ОКП и местным законодательством. LC C DP также должен проинформировать компетентный орган по защите данных о таком противоречии и вместе с органом по защите данных и компанией-участником должен искать практическое решение, максимально приближающееся к принципам Директивы ЕС о защите данных 95/46/EC.

9. Ответственность

Siemens AG берет на себя ответственность за несоблюдение ОКП компаниями-участниками, учрежденными за пределами ЕЭЗ. Siemens AG обязуется контролировать соблюдение ОКП компаниями-участниками, учрежденными за пределами ЕЭЗ, и обеспечивать, чтобы компании-участники, учрежденные за пределами ЕЭЗ, предпринимали необходимые корректирующие действия для устранения нарушений ОКП.

Siemens AG также обязуется выплатить компенсацию за ущерб в случае доказанного нарушения ОКП и, как следствие, нарушения прав субъекта данных.

Бремя доказывания лежит на Siemens AG. Siemens AG должна доказать, что нарушение ОКП не имело места, или что компания-участник, учрежденная за пределами ЕЭЗ, не несет ответственности за нарушение ОКП, в связи с которым было подано требование субъекта данных о возмещении ущерба.

SIEMENS

10. Контактное лицо

Субъекты данных могут обращаться по любым вопросам к сотруднику соответствующей компании-участника, ответственному за защиту данных (DPO), или в отдел по глобальной защите персональных данных Siemens AG:

Siemens AG

LC CO DP

St.-Martin-Str. 76

D-81541 Munich

Эл. почта: datenschutz@siemens.com

Интернет: http://www.siemens.com