СОГЛАСОВАНО

Генеральный директор
ООО «Единый оператор»

Н.В. Сапогов
_____
(подпись)
«____» _____ 20___ г.

УТВЕРЖДАЮ

Директор
ООО «Лад»

А.И. Свистунов
_____
(подпись)
«____» _____ 20____г.

П О Л О Ж Е Н И Е

об обработке и обеспечению безопасности персональных данных в Обществе с ограниченной ответственностью «Клиника имплантологии и реконструктивной хирургии «Лад»

Тюмень – 2015

Оглавление

1. Общие положения

Настоящее Положение разработано в соответствии с Конституцией РФ, Трудовым кодексом РФ № 197-ФЗ от 30.12.2001 г., Федеральным законом РФ «Об информации, информационных технологиях и о защите информации» № 149-ФЗ от 27.07.2006 г., Федеральным законом РФ «О персональных данных» № 152-ФЗ от 27.07.2006 г., Указом Президента РФ «Об утверждении перечня сведений конфиденциального характера» № 188 от 06.03.1997 г. и другими нормативными и правовыми актами, регулирующими процессы обработки персональных данных (далее – ПДн).

Настоящее Положение определяет порядок обработки и защиты персональных данных в ООО «Лад» (далее – Организация).

Персональные данные, обрабатываемые в Организации, отнесены к сведениям конфиденциального характера.

Все изменения в Положение вносятся приказом.

Все работники Организации должны быть ознакомлены с настоящим Положением, что должно быть оформлено документально.

Режим конфиденциальности персональных данных в Организации снимается в случаях их обезличивания и в соответствии со следующими сроками хранения: для персональных данных субъектов, с которыми имеются договорные отношения, срок хранения документов составляет минимум 3 года.

2. Состав, обрабатываемых персональных данных

2.1. В ИСПДн «1С: Бухгалтерский и кадровый учет» обрабатываются ПДн работников ООО «Лад»:

- фамилия, имя, отчество
- дата рождения
- серия и номер документа удостоверяющего личность (паспорт; свидетельство о рождении; военный билет;)
- дата и кем выдан и код подразделения паспорта
- место регистрации по месту жительства
- пол
- СНИЛС
- номер телефона
- место работы
- социальное положение

2.2. В ИСПДн «Медицинские автоматизированные системы» обрабатываются ПДн субъектов, не являющихся сотрудниками ООО «Лад» (клиенты и их законные представители):

- фамилия, имя, отчество
- пол
- дата рождения
- номер телефона
- место жительства
- даты оказания услуг
- стоимость лечения (*код услуги, наименование услуги*)
- история оказания услуг (проведенное лечение, результаты обследования)
- наличие/отсутствие задолжностей
- номер медицинского полиса

3. Принципы обработки персональных данных

3.1. Обработка персональных данных в Организации осуществляется на основе следующих принципов:

- законности целей и способов обработки персональных данных и добросовестности;
- соответствия целей обработки персональных данных целям, заранее определенным и заявленным при сборе персональных данных, а также полномочиям Организации;
- соответствия объема и характера обрабатываемых персональных данных, способов обработки персональных данных целям обработки персональных данных;
- достоверности персональных данных, их достаточности для целей обработки, недопустимости обработки персональных данных, избыточных по отношению к целям, заявленным при сборе персональных данных;
- недопустимости объединения созданных для несовместимых между собой целей баз данных информационных систем персональных данных.

3.2. Хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели их обработки. Персональные данные подлежат уничтожению по достижению целей обработки или в случае утраты необходимости в их достижении.

3.3. Субъект персональных данных является собственником своих персональных данных и самостоятельно решает вопрос передачи Организации своих персональных данных.

3.4. Держателем персональных данных является Организация, которой субъект персональных данных добровольно передает во владение свои персональные данные. Организации выполняет функцию владения этими данными и обладает полномочиями распоряжения ими в пределах, установленных законодательством.

3.5. Потребителями (пользователями) персональных данных являются юридические и физические лица, обращающиеся к собственнику и (или) держателю персональных данных за получением необходимых сведений и пользующиеся ими без права передачи, разглашения.

3.6. Получение, хранение, комбинирование, передача или любое другое использование персональных данных субъекта персональных данных может осуществляться исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, содействия в трудоустройстве, обучении и продвижении по службе, обеспечения личной безопасности работников и обучающихся, контроля количества и качества выполняемой работы и обеспечения сохранности имущества.

3.7. Обработка персональных данных сотрудников Организации осуществляется исключительно с целью ведения бухгалтерского и кадрового учета для обеспечения соблюдения норм Трудового Кодекса РФ и иных нормативно правовых актов.

4. Требования к обработке и защите персональных данных, обрабатываемых без использования средств автоматизации

4.1. Требования к неавтоматизированной обработке ПДн

Обработка персональных данных, содержащихся в информационной системе персональных данных либо извлеченных из такой системы, считается осуществленной *без использования средств автоматизации (неавтоматизированной)*, если такие действия с персональными данными, как использование, уточнение, распространение, уничтожение персональных данных в отношении каждого из субъектов персональных данных, осуществляются *при непосредственном участии человека*.

Персональные данные при их обработке, осуществляемой без использования средств автоматизации, должны обособляться от иной информации, в частности путем фиксации их на отдельных материальных носителях персональных данных (далее - материальные носители), в специальных разделах или на полях форм (бланков).

При фиксации персональных данных на материальных носителях не допускается фиксация на одном материальном носителе персональных данных, цели обработки которых заведомо не совместимы. Для обработки различных категорий персональных данных, осуществляемой без использования средств автоматизации, для каждой категории персональных данных должен использоваться отдельный материальный носитель.

Лица, осуществляющие обработку персональных данных без использования средств автоматизации, должны быть ознакомлены с данным Положением, и должны соблюдать правила неавтоматизированной обработки ПДн.

При использовании типовых форм документов, характер информации в которых предполагает или допускает включение в них персональных данных (далее - типовая форма), должны соблюдаться следующие условия:

a) типовая форма или связанные с ней документы (инструкция по ее заполнению, карточки, реестры и журналы) должны содержать сведения о цели обработки персональных данных, осуществляемой без использования средств автоматизации, имя (наименование) и адрес Организации, фамилию, имя, отчество и адрес субъекта персональных данных, источник получения персональных данных, сроки обработки персональных данных, перечень действий с персональными данными, которые будут совершаться в процессе их обработки, общее описание используемых Организацией способов обработки персональных данных;
b) типовая форма должна предусматривать поле, в котором субъект персональных данных может поставить отметку о своем согласии на обработку персональных данных, осуществляемую без использования средств автоматизации, - при необходимости получения письменного согласия на обработку персональных данных;
c) типовая форма должна быть составлена таким образом, чтобы каждый из субъектов персональных данных, содержащихся в документе, имел возможность ознакомиться со своими персональными данными, содержащимися в документе, не нарушая прав и законных интересов иных субъектов персональных данных;
d) типовая форма должна исключать объединение полей, предназначенных для внесения персональных данных, цели обработки которых заведомо не совместимы.

При несовместимости целей обработки персональных данных, зафиксированных на одном материальном носителе, если материальный носитель не позволяет осуществлять обработку персональных данных отдельно от других зафиксированных на том же носителе персональных данных, должны быть приняты меры по обеспечению раздельной обработки персональных данных, в частности:

a) при необходимости использования или распространения определенных персональных данных отдельно от находящихся на том же материальном носителе других персональных данных осуществляется копирование персональных данных, подлежащих распространению или использованию, способом, исключающим одновременное копирование персональных данных, не подлежащих распространению и использованию, и используется (распространяется) копия персональных данных;
b) при необходимости уничтожения или блокирования части персональных данных уничтожается или блокируется материальный носитель с предварительным копированием сведений, не подлежащих уничтожению или блокированию, способом, исключающим одновременное копирование персональных данных, подлежащих уничтожению или блокированию.

Уничтожение или обезличивание части персональных данных, если это допускается материальным носителем, может производиться способом, исключающим дальнейшую обработку этих персональных данных с сохранением возможности обработки иных данных, зафиксированных на материальном носителе (удаление, вымарывание).

Уточнение персональных данных при осуществлении их обработки без использования средств автоматизации производится путем обновления или изменения данных на материальном носителе, а если это не допускается техническими особенностями материального носителя, - путем фиксации на том же материальном носителе сведений о вносимых в них изменениях либо путем изготовления нового материального носителя с уточненными персональными данными.

4.2. Требования к защите ПДн, обрабатываемых без использования средств автоматизации

К обработке персональных данных, осуществляемой без использования средств автоматизации, допускаются сотрудники Организации, указанные в «Списке лиц, осуществляющих неавтоматизированную обработку персональных данных», утвержденном руководителем Организации.

Обработка персональных данных, осуществляемая без использования средств автоматизации, может осуществляться только в помещениях, определенных приказом руководителем Организации.

Для ПДн обработка которых, осуществляется без использования средств автоматизации, необходимо обеспечивать раздельное хранение персональных данных (материальных носителей), обработка которых осуществляется в различных целях.

Материальные носители ПДн должны сохраняться в местах, где можно обеспечить сохранность персональных данных и исключающие несанкционированный к ним доступ (сейфы, закрываемые шкафы, помещения, доступ к которым ограничен).

В соответствии с планом проверок системы защиты персональных данных, утвержденным руководителем Организации, ответственный по защите персональных данных в Организации выполняет проверку актуальности списка лиц, осуществляющих неавтоматизированную обработку персональных данных и помещений, в которых обрабатываются ПДн.

5. Требования к обработке и защите ПДн, обрабатываемых в информационных системах персональных данных Организации

Обработка персональных данных – это получение, хранение, комбинирование, передача или любое другое использование персональных данных.

Контроль выполнения требований по защите персональных данных в Организации возложен на *ответственного по защите информации в ИСПДн*. Все документы, регулирующие требования по защите ПДн, в Организации утверждаются непосредственно руководителем Организации.

Передача ПДн может быть осуществлена в органы государственного управления РФ при условии наличия официального запроса, удостоверяющего цели и основные требования, какие персональные данные необходимы, при наличии согласия субъекта ПДн на передачу своих персональных данных или без такого согласия в случаях, установленных законодательством.

Передача персональных данных при иных условиях в другие организации может быть осуществлена только при наличии правового или иного основания на передачу, не противоречащего законодательству РФ.

5.1. Обработка персональных данных субъектов ИСПДн «1С: Бухгалтерский и кадровый учет»

5.1.1. Основание для обработки персональных данных.

Обработка персональных данных в ИСПДн «1С: Бухгалтерский и кадровый учет» производится на основании ст.ст. 85-90 Трудового Кодекса РФ, Устава Организации, локальных актов Организации.

5.1.2. Цели обработки ПДн

ПДн работников Организации используются для ведения кадрового и бухгалтерского учета в соответствии с законодательством РФ.

5.1.3. Согласие на обработку ПДн

В соответствии со ст. 6 ФЗ № 152-ФЗ «О персональных данных» для обработки ПДн субъектов ИСПДн «1С: Бухгалтерский и кадровый учет» и передачи этих данных в другие организации требуется получения согласия от субъектов ПДн.

5.1.4. Получение ПДн

Персональные данные работников могут быть получены от самого работника, (субъекта, его официального представителя), либо при наличии письменного согласия на передачу ПДн от других организаций.

5.1.5. Хранение персональных данных

Часть персональных данных хранится на бумажных носителях, часть – в электронном виде в информационной системе персональных данных «1С: Бухгалтерский и кадровый учет», и распечатываются на бумажный носитель.

При хранении персональных данных принимаются меры по обеспечению их конфиденциальности в соответствии с требования ФЗ «О персональных данных», включая следующие меры: строго ограниченный доступ сотрудников к базе персональных данных на основании внутренних приказов и регламентов; обеспечение охраны помещений с базами персональных данных; предоставление доступа к базе данных по паролю; использование средств защиты от несанкционированного доступа на компьютерах, где обрабатываются персональные данные; использование средств межсетевого экранирования при передаче информации по сети.

При окончании срока обработки персональных данных субъекта, персональные данные должны удаляться из информационной системы персональных данных с составлением акта об удалении записей.

5.1.6. Места передачи ПДн

- СБИС+
- Банк-клиент ЗапСибКомБанка
- Отделение Пенсионного Фонда РФ по Тюменской области
- Федеральная налоговая служба
- Пенсионный Фонд Российской Федерации

5.2. Обработка персональных данных субъектов ИСПДн «Медицинские автоматизированные системы»

5.2.1. Основание для обработки персональных данных.

Обработка персональных данных в ИСПДн «Медицинские автоматизированные системы» производится на основании Устава Организации, локальных актов Организации.

5.2.2. Цели обработки ПДн

ПДн клиентов Организации и/или их законных представителей используются для ведения медицинской документации, оказания платных медицинских услуг.

5.2.3. Согласие на обработку ПДн

В соответствии со ст. 6 ФЗ № 152-ФЗ «О персональных данных» для обработки ПДн субъектов ИСПДн «Медицинские автоматизированные системы» и передачи этих данных в другие организации требуется получения согласия от субъектов ПДн.

5.2.4. Получение ПДн

Персональные данные субъектов могут быть получены от самих субъектов персональных данных или от их законных представителей, либо при наличии письменного согласия на передачу ПДн от других организаций.

5.2.5. Хранение персональных данных

Часть персональных данных хранится на бумажных носителях, часть – в электронном виде в информационной системе персональных данных «Медицинские автоматизированные системы», и распечатываются на бумажный носитель.

При хранении персональных данных принимаются меры по обеспечению их конфиденциальности в соответствии с требования ФЗ «О персональных данных», включая следующие меры: строго ограниченный доступ сотрудников к базе персональных данных на основании внутренних приказов и регламентов; обеспечение охраны помещений с базами персональных данных; предоставление доступа к базе данных по паролю; использование средств защиты от несанкционированного доступа на компьютерах, где обрабатываются персональные данные; использование средств межсетевого экранирования при передаче информации по сети.

При окончании срока обработки персональных данных субъекта, персональные данные должны удаляться из информационной системы персональных данных с составлением акта об удалении записей.

5.2.6. Места передачи ПДн

- Федеральная служба по надзору в сфере здравоохранения
- Департамент здравоохранения Тюменской области

5.3. Доступ к персональным данным

Доступ к персональным данным имеют сотрудники Организации, которым персональные данные необходимы в связи с исполнением ими трудовых обязанностей согласно утвержденному списку лиц доступа к ПДн.

В целях выполнения порученного задания и на основании служебной записки с положительной резолюцией руководителя Организации, доступ к персональным данным работника может быть предоставлен иному работнику, должность которого не включена в список лиц, имеющих доступ к персональным данным работника Организации, и которым они необходимы в связи с исполнением трудовых обязанностей.

В исключительных случаях, исходя из договорных отношений с контрагентом, допускается наличие в договорах пунктов о неразглашении конфиденциальной информации, в том числе предусматривающих защиту персональных данных.

Процедура оформления доступа к персональным данным включает в себя:

- ознакомление сотрудники Организации с настоящим Положением и документальное оформление факта ознакомления.
- истребование с сотрудника письменного обязательства о соблюдении конфиденциальности персональных данных и соблюдении правил их обработки.

Сотрудники работодателя, имеющие доступ к персональным данным, имеют право получать только те персональные данные, которые необходимы им для выполнения конкретных трудовых функций.

Допуск к персональным данным других сотрудников Организации, не имеющих надлежащим образом оформленного доступа, *запрещается*.

Субъект имеет право на свободный доступ к своим персональным данным, включая право на получение копии любой записи (за исключением случаев, предусмотренных федеральным законом), содержащей его персональные данные. Субъект имеет право вносить предложения по внесению изменений в свои данные в случае обнаружения в них неточностей.

При передаче персональных данных Субъекта, сотрудники Организации предупреждают лиц, получающих данную информацию, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и истребуют от этих лиц письменное обязательство.

Передача (обмен и т.д.) персональных данных между подразделениями Организации осуществляется только между сотрудниками, имеющими доступ к персональным данным.

Передача персональных данных третьим лицам осуществляется только с письменного согласия субъекта ПДн, которое оформляется по установленной форме и должно включать в себя:

- фамилию, имя, отчество, адрес субъекта ПДн, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;
- наименование и адрес Организации, получающего согласие субъекта ПДн;
- цель передачи персональных данных;
- перечень персональных данных, на передачу которых дает согласие субъекта ПДн;
- перечень действий с персональными данными, на совершение которых дается согласие;
- срок, в течение которого действует согласие, а также порядок его отзыва.

Согласия субъекта ПДн на передачу его персональных данных третьим лицам не требуется в случаях, когда это необходимо в целях предупреждения угрозы жизни и здоровью субъекта ПДн, а также в случаях, установленных федеральным законом и настоящим Положением.

Не допускается передача персональных данных субъекта ПДн в коммерческих целях без его письменного согласия.

Представителю субъекта ПДн (в том числе адвокату) персональные данные передаются в порядке, установленном действующим законодательством и настоящим Положением.

Предоставление персональных данных субъекта ПДн государственным органам производится в соответствии с требованиями действующего законодательства и настоящего Положения.

Персональные данные субъекта ПДн могут быть предоставлены родственникам или членам его семьи только с письменного разрешения самого субъекта ПДн, за исключением случаев, когда передача персональных данных работника без его согласия допускается действующим законодательством РФ.

Документы, содержащие персональные данные субъекта ПДн, могут быть отправлены через организацию федеральной почтовой связи. При этом должна быть обеспечена их конфиденциальность. Документы, содержащие персональные данные вкладываются в конверт, к нему прилагается сопроводительное письмо. На конверте делается надпись о том, что содержимое конверта является конфиденциальной информацией, и за незаконное ее разглашение законодательством предусмотрена ответственность. Далее, конверт с сопроводительным письмом вкладывается в другой конверт, на который наносятся только реквизиты, предусмотренные почтовыми правилами для заказных почтовых отправлений.

При организации доступа к персональным данным лицам, не являющихся сотрудниками Организации, необходимо выполнение всех требований по обеспечению безопасности, установленных для сотрудников Организации.

6. Общий порядок организации работ по обеспечению безопасности ПДн при их обработке в ИСПДн

Обеспечением безопасности персональных данных в Организации занимаются Ответственные по защите информации в ИСПДн.

Все персональные данные, обрабатываемые в Организации, храниться на материальных носителях, список которых утвержден руководителем Организации. Хранение и передача персональных данных на других носителях информации, может осуществляться только с разрешения руководства Организации.

Каждый сотрудник Организации перед обработкой персональных данных должен ознакомиться и подписать соглашение о конфиденциальности персональных данных, с которым он будет работать (соглашение может подписываться, как часть других документов, например, трудовых инструкций).

Для обеспечения безопасности персональных данных при их обработке в Организации каждый сотрудник обязан выполнять требования, указанные в соглашении о конфиденциальности, и не использовать персональные данные, к которым он получил доступ в процессе исполнения трудовых обязанностей для целей не связанных с исполнением его трудовых обязанностей.

Каждый сотрудник Организации при передаче ПДн другим сотрудникам Организации должен контролировать, наличие доступа у принимающего сотрудника на обработку персональных данных.

При увольнении сотрудники Организации должны передавать все обрабатываемые ими персональные данные, находящие на бумажных и электронных носителях информации, своим непосредственным начальникам.

6.1. Порядок обработки инцидентов нарушения безопасности персональных данных

Под *инцидентом информационной безопасности* будем понимать событие, являющееся следствием одного или нескольких нежелательных или неожиданных событий ИБ, имеющих значительную вероятность компрометации ПДн одного или нескольких субъектов.

Каждый пользователь ИСПДн при обнаружении инцидента безопасности, относящегося к персональным данным должен сообщить о данном факте ответственному по защите персональных данных или руководству Организации, и в дальнейшем содействовать информационным и иными способами успешному расследованию данного инцидента.

При обнаружении нарушения характеристик безопасности ИСПДн пользователи обязаны приостановить обработку ПДн до выявления причин нарушений и их устранения.

В Организации для обработки инцидентов безопасности персональных данных создана группа реагирования на инциденты безопасности персональных данных, в состав которой входят:

- ответственный за организацию обработки ПДн;
- ответственный по защите информации в ИСПДн;
- администратор безопасности ИСПДн.

Работа группы реагирования регламентируется инструкциями по обработке инцидентов безопасности, утвержденным руководством Организации.

Общая схема обработки инцидентов выглядит следующим образом:

1. Пользователь ИСПДн обнаружил инцидент;

2. Пользователь оповещает группу реагирования на инциденты безопасности ПДн;
3. Сотрудник группы реагирования на инциденты на базе информации пользователя составляет отчет по факту заявки пользователя;
4. При подтверждении наличия инцидента безопасности ПДн сотрудник группы реагирования на инциденты производит детальный сбор информации и анализ результатов инцидента;
5. Далее вырабатывается план обработки инцидента безопасности;
6. После исполнения действий по плану обработки инцидента, специалист группы реагирования на инциденты выполняет анализ эффективности предпринятых действий, при необходимости повторяется действия с шага 4;
7. Специалист группы реагирования на инциденты составляет отчет об обработке инцидента безопасности ПДн.

Если в результате анализа инцидента определенно, что информация о субъектах ПДн не является точной и/или не доступна, то *пользователи ИСПДн должны прекратить обработку ПДн этого субъекта до разрешения инцидента группой реагирования на инциденты безопасности ПДн*, и при необходимости проинформировать субъекта ПДн о невозможности предоставления услуги обработки ПДн.

Инциденты безопасности ПДн обрабатываются по мере загруженности специалистов группы реагирования на инциденты, максимально в *срок 5 рабочих дней*.

6.2. Порядок обучения администраторов и пользователей ИСПДн

Все пользователи ИСПДн проходят ознакомление с правилами безопасной работы с ПДн перед началом обработки ПДн, указанные в данном Положении и инструкциях по обеспечению безопасности при работе в ИСПДн. Пользователи ИСПДн проходят обучение по вопросам обеспечения защиты ПД каждые *2 года* и проходят аттестацию на знание регламентов и инструкций каждый *год*.

Каждый пользователь ИСПДн обязан соблюдать требования по обеспечению безопасности ПДн указанные в регламентах и инструкциях, при невыполнении требований по защите ПДн, пользователь ИСПДн допустивший реализацию угрозы безопасности ПДн несет уголовную, административную и иные виды ответственностей в соответствии с действующим законодательством и ответственность, указанную в регламентах и требованиях по защите информации.

Администраторы информационной безопасности проходят обучение по вопросам обеспечения безопасности ПДн каждые *3 года* или чаще. *Каждый год* администраторы ИБ проходят аттестации знаний по обеспечению безопасности информации. Администраторы ИБ в обязательном порядке до осуществления своих непосредственных обязанностей должны ознакомиться и подписать регламенты и инструкции по работе с ИСПДн и со средствами защиты информации. Администраторы ИБ несут ответственность, указанную в регламентах и инструкциях, за не правильную настройку средств защиты информации (не соответствующую регламентам) повлекшую в итоге реализацию одной или нескольких угроз безопасности информации.

Администраторы информационных систем и другие пользователи, имеющие доступ к ИСПДн, перед началом работы с ИСПДн должны ознакомиться и подписать инструкции и регламенты по обеспечению безопасности ПДн. При несоблюдении требований по обеспечению безопасности ПДн администраторы информационных систем и другие пользователи, имеющие доступ к ИСПДн, несут ответственность, указанную в регламентах и инструкциях, за не правильную настройку средств защиты

информации (не соответствующую регламентам) повлекшую в итоге реализацию одной или нескольких угроз безопасности информации.

6.3. Порядок организации ведения и периодической проверки электронного журнала обращений пользователей информационной системы к ПДн

Список всех пользователей ИСПДн обрабатывающих ПДн должен быть закреплен документально и утвержден руководством Организации.

Списки пользователей ИСПДн по мере изменения их содержания должны актуализироваться и также утверждаться руководством Организации.

Матрица доступа пользователей ИСПДн к ПДн должна быть актуальной относительно наличия прав доступа пользователей к защищаемой информации. Каждые *6 месяцев* должна проводиться проверка актуальности записей, указанных в матрице доступа реально назначенным разрешениям пользователей ИСПДн к ПДн.

Обращение пользователей ИСПДн к ПДн должно фиксироваться в электронном журнале обращений для возможности его периодической проверки администраторами безопасности.

7. Ответственность за нарушение норм, регулирующих обработку и защиту персональных данных работника

Руководитель, разрешающий доступ сотрудника к конфиденциальному документу, содержащему персональные данные, несет персональную ответственность за данное разрешение.

Каждый сотрудник Организации, получающий для работы конфиденциальный документ, несет единоличную ответственность за сохранность носителя и конфиденциальность информации.

Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных, привлекаются к дисциплинарной и материальной ответственности в порядке, установленном Трудовым Кодексом Российской Федерации и иными федеральными законами, а также привлекаются к гражданско-правовой, административной и уголовной ответственности в порядке, установленном федеральными законами.

Согласие о неразглашении
Персональных данных

Я, _____, паспорт серии _____, номер _____, выданный _____ «___» _____ _____ года, понимаю, что получаю доступ к персональным данным сотрудников _____; клиентов и их законных представителей_____ (нужное подчеркнуть).

Я также понимаю, что во время исполнения своих обязанностей, мне приходится заниматься сбором, обработкой и хранением персональных данных.

Я понимаю, что разглашение такого рода информации может нанести ущерб Организации, как прямой, так и косвенный.

В связи с этим, даю обязательство, при работе (сбор, обработка и хранение) с персональными данными соблюдать требования, описанные в «Положении об обработке и обеспечению безопасности персональных данных» и других документах Организации, регулирующих вопросы защиты ПДн в Организации.

Я подтверждаю, что не имею права разглашать персональные данные, полученные мною в результате трудовой деятельности.

Я предупрежден (а) о том, что в случае разглашения мной сведений, касающихся персональных данных или их утраты я несу ответственность в соответствии со статьями 13.11, 13.12, 13.14 кодекса РФ об административных правонарушениях, статьями 137, 138, 272, 273, 274 уголовного кодекса РФ, статьей 90 трудового кодекса РФ и иных нормативно-правовых актов РФ, а также могу быть привлечен (а) к гражданской, уголовной, административной, дисциплинарной и иной предусмотренной законодательством Российской Федерации ответственности.

« _____ » _____ 20__ г.

_____
(подпись)

Уч. № 06ДСП
Отп. в ед.экз. на 16 листах
Исп. А.И. Свистунов, отп. А.И. Свистунов
Тел. 47-67-83
18.02.2015 г.