



УТВЕРЖДЕНО

Генеральный директор
Юнусова Г.Ф.
«20» апреля 2023 года

Положение о работе с персональными данными ООО «Центр лазерной и эстетической медицины»

Общие положения

Настоящее Положение о работе с персональными данными (далее - Положение), определяет политику ООО «Центр лазерной и эстетической медицины» (далее – Организация или Оператор) в области обработки персональных данных, основные принципы, содержит сведения о реализуемых мерах по защите, порядок работы и условиях обработки персональных данных в отношении:

- физических лиц, получающих медицинскую помощь в Организации на основании договора на оказание платных медицинских услуг (далее – Пациент или Субъект ПД);
- физических лиц, представляющих интересы Пациентов (далее – Представитель или Субъект ПД);
- физических лиц, являющиеся клиентами, потенциальными клиентами Организации и/или заинтересованные в получении информации, связанной с деятельностью Организации (далее – Пользователь, Клиент или Субъект ПД).

Положение разработано в целях реализации требований законодательства в области обработки и защиты персональных данных, и направлена на обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных в Организации, в том числе защиты прав на неприкосновенность частной жизни, личной, семейной и врачебной тайн.

Настоящее Положение вступает в силу с момента его утверждения руководителем Организации и действует бессрочно, до замены его новым Положением. Все изменения в Положение вносятся приказом.

Положение размещается на информационном стенде в холле Организации по адресу: Республика Татарстан город Набережные Челны, улица Шамиля Усманова, дом 17, корпус 3, а электронная версия Положения – на сайте <http://lcode-clinic.ru/>. По всем вопросам, касающимся обработки персональных данных, можно обратиться по телефону Организации (8552)913-213 и на электронную почту по адресу lcode.chelny@gmail.com.

Положение является обязательным для исполнения всеми работниками Оператора, имеющими доступ к персональным данным, и действует в отношении всех персональных данных, которые Оператор может получить от Субъекта персональных данных (далее – Субъект ПД).

Настоящее Положение разработано в соответствии с Федеральным законом №152-ФЗ от 27.07.2006г «О персональных данных», Федеральным законом от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации», Разъяснения Роскомнадзора "О вопросах отнесения фото- и видео- изображения, дактилоскопических данных и иной информации к биометрическим персональным данным и особенности их обработки" и другими нормативно-правовыми актами РФ в области защиты персональных данных.

Термины и принятые сокращения

- Персональные данные (ПД) – любая информация, относящаяся к прямо или косвенно определенному, или определяемому физическому лицу (субъекту персональных данных).
- Обработка персональных данных – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование,

передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

- Оператор – государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.
- Распространение персональных данных – действия, направленные на раскрытие персональных данных неопределенному кругу лиц.
- Предоставление персональных данных – действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц.
- Блокирование персональных данных – временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных).
- Уничтожение персональных данных – действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных.
- Обезличивание персональных данных – действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.
- Автоматизированная обработка персональных данных – обработка персональных данных с помощью средств вычислительной техники.
- Информационная система персональных данных (ИСПД) – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.
- Пациент – физическое лицо, которому оказывается медицинская помощь или которое обратилось за оказанием медицинской помощи, консультацией независимо от наличия у него заболевания и от его состояния.

Принципы обработки персональных данных

Обработка персональных данных осуществляется на законной и справедливой основе.

Обработка персональных данных ограничивается достижением конкретных, заранее определенных и законных целей. Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных.

Не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой.

Обработке подлежат только персональные данные, которые отвечают целям их обработки.

Содержание и объем обрабатываемых персональных данных соответствуют заявленным целям обработки. Не допускается избыточность обрабатываемых персональных данных по отношению к заявленным целям их обработки.

При обработке персональных данных обеспечивается точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки персональных данных. Оператор принимает необходимые меры и/или обеспечивает их принятие по удалению или уточнению неполных или неточных данных.

Хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных. Обрабатываемые персональные данные подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

Условия обработки персональных данных

Обработка персональных данных осуществляется с согласия Субъекта ПД на обработку его персональных данных. Все персональные данные о Субъекте ПД Оператор получает от него самого либо его законного (уполномоченного) представителя.

Субъект ПД знакомится и соглашается с условиями настоящего Положения и даёт согласие на обработку своих персональных данных, совершая следующие действия:

- подписывая Согласие на обработку персональных данных;
- подписывая Согласие на распространение персональных данных;
- нажимая на кнопку «Отправить», «Написать нам» и/или «Заказать звонок» в форме обратной связи, расположенной на официальном сайте Организации <http://lcode-clinic.ru>;
- нажимая кнопку «Записаться» в форме обратной связи в заявке на предварительную запись на приём в приложении CRM Малахит;
- используя сайт <http://lcode-clinic.ru>, Пользователь, даёт свое согласие на использование cookie-файлов. Пользователь может отказаться от использования или заблокировать все или определенные cookie-файлы в своем браузере, однако, в таком случае, работа отдельных элементов сайта может быть нарушена.

Посетители Организации заранее предупреждаются администрацией о видеосъёмке соответствующими текстовыми и/или графическими предупреждениями. При соблюдении указанного условия согласие Субъектов на проведение видеосъёмки не требуется. Видеонаблюдение в помещениях Организации ведётся с целью обеспечения безопасности, фиксации возможных действий противоправного характера.

Предоставленное Субъектом ПД Согласие на обработку персональных данных действует со дня предоставления такого согласия и в течение срока, необходимого для достижения целей обработки персональных данных или до момента отзыва Субъектом ПД указанного согласия, если иное не предусмотрено действующим законодательством РФ.

Предоставленное Субъектом ПД Согласие на обработку ПД может быть в любой момент отозвано Субъектом ПД. Субъект ПД может отозвать предоставленное ранее Организации согласие на обработку ПД следующим способом:

- предъявив оригинал заявления лично (или через уполномоченного представителя) сотруднику Организации или отправив по почте заказным письмом по адресу: 423822, Республика Татарстан, город Набережные Челны, улица Шамиля Усманова, дом 17, корпус 3.

В случае отзыва Субъектом ПД Согласия на обработку персональных данных, Оператор вправе продолжить обработку персональных данных без согласия Субъекта ПД при наличии оснований, указанных в пунктах 2–11 части 1 статьи 6, части 2 статьи 10 и части 2 статьи 11 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».

Вся информация, которая собирается сторонними сервисами, в том числе платежными системами, средствами связи и другими поставщиками услуг, хранится и обрабатывается указанными лицами (Операторами) в соответствии с их Пользовательским соглашением и Политикой конфиденциальности. Оператор не несет ответственность за действия третьих лиц, в том числе указанных в настоящем пункте поставщиков услуг.

Порядок обработки персональных данных

Цель обработки персональных данных. Персональные данные Субъектов ПД обрабатываются с целью:

- оказания населению платных медицинских услуг в соответствии с Федеральным законом от 21.11.2011 г. №323-ФЗ «Об основах охраны здоровья граждан Российской Федерации», Правилами предоставления медицинскими организациями платных медицинских услуг, утвержденными постановлением Правительства РФ от 4 октября 2012 г. № 1006;
- информирования и консультирования населения об оказываемых Организацией услугах, продаваемых товарах, условиях и порядке их предоставления (приобретения);

- осуществления предварительной записи на приём и уведомления о дате и времени предстоящего визита;
- идентификации личности Субъекта ПД;
- поддержания связи с Пациентами и ознакомления их с изменениями в работе Организации, с действующими акциями, специальными предложениями, другой информацией;
- осуществление гражданско-правовых отношений;
- улучшения качества обслуживания, путём обработки запросов, отзывов, поступивших от Субъектов ПД;
- обеспечения корректной работы сайта <http://lcode-clinic.ru>;
- проведения веб-аналитики с целью улучшения и оптимизации работы сайта <http://lcode-clinic.ru>.

Персональные данные в Организации обрабатываются вручную на бумажных носителях и автоматизированным способом с использованием средств вычислительной техники.

Документы, содержащие персональные данные, создаются в процессе:

- Заполнения анкет;
- Подписания договора на оказание платных медицинских услуг;
- Заполнение работником Организации медицинской карты Пациента;
- Создание иных документов и учётных форм в процессе обращения в Организацию и получения услуг в Организации;
- Заполнение форм обратной связи на официальном сайте Организации, CRM Малахит.

Перечень персональных данных, обрабатываемых Оператором:

- Фамилия, Имя, Отчество
- Дата рождения
- Реквизиты документа, удостоверяющего личность
- Реквизиты документа, дающего право на представление интересов Пациента
- Адрес регистрации и места пребывания
- Номера телефонов
- E-mail
- Данные о состоянии здоровья, имеющихся заболеваниях и назначенном лечении
- Изображение (фотография) «до» и «после» медицинских вмешательств
- Изображения с камер видеонаблюдения, осуществляющих запись голоса и изображения
- Технические и аналитические файлы cookie. Информация, собранная при помощи файлов cookie на сайте Организации: IP-адрес Пользователя, дата и время посещения сайта, браузер и его версия, операционная система и ее версия, тип и модель устройства, источник входа на сайт, информация о поведении Пользователя на сайте (включая количество и наименование просмотренных страниц).

Действия, совершаемые с персональными данными:

- сбор;
- запись;
- систематизация;
- накопление;
- хранение;
- уточнение (обновление, изменение);
- извлечение;
- использование;
- передача (распространение, предоставление, доступ);
- обезличивание;
- блокирование;
- удаление;
- уничтожение.

Хранение и уничтожение персональных данных. Хранение персональных данных осуществляется на бумажных носителях (медицинские карты, договоры, согласие на обработку персональных данных, анкеты, другие документы), которые хранятся в закрываемом помещении, с

ограниченным правом доступа. В электронном виде персональные данные обрабатываются и хранятся в CRM Малахит.

Персональные данные посетителей Организации, полученные при помощи камер видеонаблюдения, хранятся на локальном сервере Организации в течение 45 календарных дней.

Срок хранения медицинской карты Пациента, получающего медицинскую помощь в амбулаторных условиях - составляет 25 лет. Срок хранения договора на оказание платных медицинских услуг - 3 года.

Персональные данные Субъектов ПД подлежат уничтожению:

- по истечении срока хранения архивных документов;
- при достижении целей обработки или в случае утраты необходимости в их достижении - в течении 30-ти дней с даты достижения цели, если иное не предусмотрено договором (соглашением);
- в случае отзыва Субъектом ПД согласия на обработку его персональных данных - в течении 30-ти дней с даты поступления отзыва. В случае отзыва Субъектом ПД Согласия на обработку персональных данных, Оператор вправе продолжить обработку персональных данных без согласия Субъекта ПД при наличии оснований, указанных в пунктах 2-11 части 1 статьи 6, части 2 статьи 10 и части 2 статьи 11 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»;
- в случае выявления неправомерной обработки персональных данных и если обеспечить правомерность обработки персональных данных невозможно, Оператор в срок, не превышающий 10-ти рабочих дней с даты выявления неправомерной обработки персональных данных, обязан уничтожить такие персональные данные.

Отбор документов, подлежащих уничтожению, осуществляет ответственное за уничтожение персональных данных лицо, назначенное руководителем Организации. Уничтожение документов организуется таким образом, чтобы исключить возможность разглашения сведений посторонним лицам. Бумажные носители персональных данных уничтожаются с помощью shreddera. Электронные файлы с персональными данными удаляются («стираются») средствами операционной системы компьютера с последующим «очищением корзины».

В акте об уничтожении носителей, содержащих персональные данные Субъектов ПД, указываются:

- дата, место и время уничтожения;
- должность, фамилия, инициалы ответственного лица за уничтожение персональных данных;
- вид и количество уничтожаемых носителей, содержащих персональные данные Субъектов ПД;
- основание для уничтожения;
- способ уничтожения.

В случае необходимости, Организация уведомляет об уничтожении персональных данных Субъект ПД и/или уполномоченный орган.

Права и обязанности субъектов персональных данных

Субъекты персональных данных имеют право:

- получать информацию, касающуюся обработки его персональных данных, за исключением случаев, предусмотренных федеральными законами. Сведения предоставляются Субъекту ПД Оператором в доступной форме, и в них не должны содержаться персональные данные, относящиеся к другим Субъектам ПД, за исключением случаев, когда имеются законные основания для раскрытия таких персональных данных. Перечень информации и порядок ее получения установлен Законом о персональных данных;
- требовать от оператора уточнения его персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав;

- на отзыв согласия на обработку персональных данных, а также, на направление требования о прекращении обработки персональных данных;
- обжаловать в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке неправомерные действия или бездействие Оператора при обработке его персональных данных;
- на осуществление иных прав, предусмотренных законодательством РФ.

Субъекты ПД обязаны:

- предоставлять Оператору достоверные данные о себе;
- сообщать Оператору об уточнении (обновлении, изменении) своих персональных данных.

Лица, передавшие Оператору недостоверные сведения о себе, либо сведения о другом Субъекте ПД без согласия последнего, несут ответственность в соответствии с законодательством РФ.

Обязанности Оператора.

Оператор при обработке персональных данных обязан:

- Назначить ответственных лиц за организацию обработки и обеспечение безопасности персональных данных, а также определить круг лиц, имеющих доступ к персональным данным в силу исполнения ими своих должностных обязанностей;
- При сборе персональных данных предоставить Субъекту ПД полную информацию об их обработке;
- В случае, если персональные данные были получены не от Субъекта ПД, уведомить Субъект ПД о получении его персональных данных;
- При отказе Субъекта ПД от предоставления персональных данных и/или согласия на их обработку, разъяснить последствия такого отказа;
- Опубликовать или иным образом обеспечить неограниченный доступ к настоящему Положению, определяющему политику Оператора в отношении обработки и защиты персональных данных;
- Принимать необходимые правовые, организационные, технические меры или обеспечивать их принятие для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении персональных данных;
- Отвечать на запросы и обращения Субъектов ПД, их представителей и/или уполномоченного органа по защите прав Субъектов ПД в течение 10 (десяти) рабочих дней с момента получения Оператором соответствующего запроса;
- Не предоставлять персональные данные Субъектов ПД третьим лицам без их согласия, за исключением случаев, предусмотренных Федеральными законами РФ;
- В случае установления факта неправомерной или случайной передачи (предоставления, распространения, доступа) персональных данных, повлекшей нарушение прав Субъектов ПД, оператор обязан с момента выявления такого инцидента уведомить Роскомнадзор: в течение 24 часов об инциденте, предполагаемых причинах и потенциальном вреде, нанесенном правам Субъектов ПД, о принятых мерах по устранению последствий соответствующего инцидента. В этот же срок предоставляются сведения об уполномоченном сотруднике, который будет взаимодействовать с уполномоченным органом по защите прав субъектов персональных данных, по вопросам, связанным с выявленным инцидентом; в течение 72 часов о результатах внутреннего расследования инцидента, а также о виновных лицах, чьи действия стали причиной инцидента.

Меры обеспечения безопасности персональных данных. Ответственность за разглашение персональных данных

Безопасность персональных данных, которые обрабатываются Оператором, обеспечивается путем реализации правовых, организационных и технических мер, необходимых для выполнения в полном объеме требований действующего законодательства в области защиты персональных данных.

Оператор обеспечивает сохранность персональных данных и принимает все возможные меры, исключающие доступ к персональным данным неуполномоченных лиц.

Сайт Организации и база данных CRM Малахит, располагаются на хостингах и серверах, находящихся на территории Российской Федерации.

Персональные данные Субъекта ПД никогда, ни при каких условиях не будут переданы третьим лицам, за исключением случаев, связанных с исполнением действующего законодательства либо в случае, если Субъектом ПД дано согласие Оператору на передачу данных третьему лицу для исполнения обязательств по гражданско-правовому договору.

Для обеспечения внешней защиты персональных данных разработаны и внедрены следующие меры безопасности:

- На входной двери установлен домофон с видеосвязью, обеспечивающий контролируемый доступ на территорию организации;
- В организации установлена система охранной сигнализации, которая обеспечивает подачу на пульт дежурному сигналов о попытке проникновения в помещение в нерабочее время;
- Для обеспечения безопасности в организации установлены камеры видеонаблюдения, охватывающие коридоры, холл, прилегающую территорию центра;
- Доступ к электронным базам данных, содержащим персональные данные работников, обеспечивается двухступенчатой системой паролей;
- Помещение оснащено системой пожарной сигнализации.

В число организационных мер защиты персональных данных входит регламентация доступа работников Организации к сведениям, документам и базам данных. Право доступа к персональным данным Субъектов ПД имеют только те работники Оператора, которым в связи с выполнением трудовой функции необходимо иметь доступ к персональным данным Субъектов ПД.

Персональные данные Пациентов относятся к категории конфиденциальной информации. Лица, получившие доступ к персональным данным, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия Субъекта ПД, если иное не предусмотрено федеральным законом.

Перечень должностей, имеющих доступ к персональным данным Субъектов ПД, утверждается Приказом руководителя Организации.

Работники Организации, имеющие доступ к персональным данным Субъектов ПД, обязуются принимать необходимые организационные и технические меры для защиты персональных данных Субъектов ПД от неправомерного или случайного доступа, уничтожения, изменения, блокирования, копирования, распространения, а также иных неправомерных действий третьих лиц.

Сотрудники, имеющие доступ к персональным данным, не должны:

- оставлять в свое отсутствие незапертым помещение, в котором хранятся персональные данные Субъектов ПД на бумажных носителях;
- оставлять на рабочем столе, в свободном доступе, без присмотра медицинские карты и другие документы, содержащие персональные данные Субъектов ПД;
- оставлять в свободном доступе, без присмотра компьютер и информационную базу, в которых содержатся персональные данные Субъектов ПД.

Сотрудник Организации, получающий для работы документ, содержащий персональные данные Субъекта ПД, несет единоличную ответственность за сохранность носителя и конфиденциальность информации.

Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных Субъектов ПД, несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность.