«УТВЕРЖДАЮ»
Генеральный директор
ООО «Калита»
_____ О.Н. Нестеренко

«_____» _____ 2017 года

Политика
обработки и защиты персональных данных
ООО «Калита»

1. Общие положения

1.1. Настоящая Политика в отношении обработки персональных данных (далее - Политика) составлена в соответствии с п. 2 ст. 18.1 Федерального закона № 152-ФЗ от 27 июля 2006 года «О персональных данных» и является основополагающим внутренним регулятивным документом Общества с ограниченной ответственностью ООО «Калита» (далее - Организация), определяющим ключевые направления его деятельности в области обработки и защиты персональных данных (далее - Данные), оператором которых является Организация.

1.2. Политика разработана в целях реализации требований законодательства в области обработки и защиты Данных и направлена на обеспечение защиты прав и свобод человека и гражданина при обработке его Данных в Организации, в том числе защиты прав на неприкосновенность частной жизни, личной, семейной и врачебной тайн.

1.3. Положения Политики распространяются на отношения по обработке и защите Данных, полученных Организацией как до, так и после утверждения Политики, за исключением случаев, когда по причинам правового, организационного и иного характера положения Политики не могут быть распространены на отношения по обработке и защиты Данных, полученных до её утверждения.

1.4. Обработка Данных в организации осуществляется в связи с выполнением Организацией функций, предусмотренных её учредительными документами, и определяемых:

- Федеральным законом от 21 ноября 2011 г. № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации»;
- Федеральным законом № 152-ФЗ от 27 июля 2006 года «О персональных данных»;
- Постановлением Правительства Российской Федерации от 15 сентября 2008 года № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации;
- Постановлением Правительства РФ от 1 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- иными нормативными правовыми актами Российской Федерации.

Кроме того, обработка Данных в Организации осуществляется в ходе трудовых и иных непосредственно связанных с ними отношений, в которых Организация выступает в качестве работодателя (глава 14 Трудового кодекса Российской Федерации), в связи с реализацией Организацией своих прав и обязанностей как юридического лица.

1.5. Организация имеет право вносить изменения в настоящую Политику. При внесении изменений в заголовке Политики указывается дата последнего обновления редакции. Новая редакция Политики вступает в силу с момента её размещения на сайте, если иное не предусмотрено новой редакцией Политики.

1.6. Действующая редакция хранится в месте нахождения Организации по адресу:

Тамбовская область, г. Тамбов, ул.Советская, д.119, № 258б, электронная версия

Политики — на сайтах по адресам: odvoptic.ru, puls68.ru

2. Термины и принятые сокращения

Персональные данные (Данные) — 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 определенному 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 уничтожения 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 контрактному 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 независимо от наличия у него заболевания и от его состояния.

Медицинская деятельность — профессиональная деятельность по оказанию медицинской помощи, проведению медицинских экспертиз, медицинских осмотров и медицинских освидетельствований, санитарно-противоэпидемических (профилактических) мероприятий и профессиональная деятельность, связанная с трансплантацией (пересадкой) органов и (или) тканей, обращением донорской крови и (или) её компонентов в медицинских целях.

Лечащий врач — врач, на которого возложены функции по организации и непосредственному оказанию пациенту медицинской помощи в период наблюдения за ним и его лечения.

3. Принципы обеспечения безопасности персональных данных

3.1 Основной задачей обеспечения безопасности Данных при их обработке в Организации является предотвращение несанкционированного доступа к ним третьих лиц,

предупреждение преднамеренно программно-технических и иных воздействий с целью хищения Данных, разрушения (уничтожения) или искажения их в процессе обработки.

3.2. Для обеспечения безопасности Данных Организация руководствуется следующими принципами:

- законность: защита Данных основывается на положениях нормативных правовых актов и методических документов уполномоченных государственных органов в области обработки и защиты Данных;
- системность: обработка Данных в Организации осуществляется с учетом всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, значимых для понимания и решения проблемы обеспечения безопасности Данных;
- комплексность: защита Данных строится с использованием функциональных возможностей информационных технологий, реализованных в информационных системах Организации и других имеющихся в Организации систем и средств защиты;
- непрерывность: защита Данных обеспечивается на всех этапах их обработки и во всех режимах функционирования систем обработки Данных, в том числе при проведении ремонтных и регламентных работ;
- своевременность: меры, обеспечивающие надлежащий уровень безопасности Данных, принимаются до начала их обработки;
- преемственность и непрерывность совершенствования: модернизация и наращивание мер и средств защиты Данных осуществляется на основании результатов анализа практики обработки Данных в Организации с учетом выявления новых способов и средств реализации угроз безопасности Данных, отечественного и зарубежного опыта в сфере защиты информации;
- персональная ответственность: ответственность за обеспечение безопасности Данных возлагается на работников в пределах их обязанностей, связанных с обработкой и защитой Данных;
- минимизация прав доступа: доступ к Данным предоставляется работникам только в объеме, необходимом для выполнения их должностных обязанностей;
- гибкость: обеспечение выполнения функций защиты Данных при изменении характеристик функционирования информационных систем персональных данных Организации, а также объема и состава обрабатываемых Данных;
- специализация и профессионализм: реализация мер по обеспечению безопасности Данных осуществляется работниками, имеющими необходимые квалификацию и опыт;
- эффективность процедур отбора кадров: кадровая политика Организации предусматривает тщательный побор персонала и мотивацию Работников, позволяющие исключить или минимизировать возможность нарушения ими безопасности Данных;
- наблюдаемость и прозрачность: меры по обеспечению безопасности Данных должны быть спланированы так, чтобы результаты их применения были явно наблюдаемы (прозрачны) и могли бы оценены лицами, осуществляющими контроль;
- непрерывность контроля и оценки: устанавливаются процедуры постоянного контроля использования систем обработки и защиты Данных, а результаты контроля регулярно анализируются.

3.3. В организации не производится обработка Данных, несовместимая с целями их сбора. Если иное не предусмотрено федеральным законом, по окончании обработки Данных в Организации, в том числе при достижении целей их обработки или утраты необходимости в достижении этих целей, обрабатывающиеся Организацией Данные уничтожаются или обезличиваются.

3.4. При обработке Данных обеспечиваются их точность, достаточность, а при необходимости — и актуальность по отношению к целям обработки. Организация принимает необходимые меры по удалению неполных или неточных Данных.

4. Обработка персональных данных

4.1 Получение Данных.

4.1.1. Все Данные следует получать от самого субъекта. Если Данные субъекта можно получить только у третьей стороны, то субъект должен быть уведомлен об этом или от него должно быть получено согласие.

4.1.2. Оператор должен сообщить субъекту о целях, предполагаемых источниках и способах получения Данных, характере подлежащих получению Данных, перечне действий с Данными, сроке, в течение которого действует согласие, и порядке его отзыва, а также о последствиях отказа субъекта дать письменное согласие на их получение.

4.1.3 Документы, содержащие Данные, создаются путем:

а) копирования оригиналов документов (паспорт, документ об образовании, свидетельство ИНН, пенсионное свидетельство и др.);

б) внесения сведений в учетные формы;

в) получение оригиналов необходимых документов (трудовая книжка, медицинское заключение, характеристика и др.)

Порядок доступа субъекта Данных к его Данным, обрабатываемым Организацией, определяется в соответствии с законодательством и внутренними регулятивными документами Организации.

4.2 Обработка Данных**.**

4.2.1 Обработка персональных данных осуществляется:

- с согласия субъекта персональных данных на обработку его персональных данных;
- в случаях, когда обработка персональных данных необходима для осуществления и выполнения возложенных законодательством Российской Федерации функций, полномочий и обязанностей;
- в случаях, когда осуществляется обработка персональных данных, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных либо по его просьбе (далее — персональные данные, сделанные общедоступными субъектом персональных данных).

Доступ работников к обрабатываемым Данным осуществляется в соответствии с их должностными обязанностями и требованиями внутренних регулятивных документов Организации.

Организацией производится устранение выявленных нарушений законодательства об обработке и защите Данных.

4.2.2 Цели обработки Данных:

- обеспечение организации оказания платных медицинских услуг населению, а также наиболее полного исполнения обязательств и компетенций в соответствии с Федеральными законами от 21 ноября 2011 г. № 323-ФЗ «Об основах охраны здоровья граждан Российской Федерации», от 12 апреля 2010 №61-ФЗ «Об обращении лекарственных средств» и Правилами предоставления медицинским организациями платных медицинских услуг, утвержденными постановлением Правительства Российской Федерации от 4 октября 2012 г. № 1006;
- осуществление трудовых отношений;
- осуществление гражданско-правовых отношений.

4.2.3 Категории субъектов персональных данных.

В Организации обрабатываются Данные следующих субъектов:

- физические лица, состоящие с учреждением в трудовых отношениях;
- физические лица, являющиеся близкими родственниками сотрудниками учреждения
- физические лица, уволившиеся из учреждения;
- физические лица, являющиеся кандидатами на работу;

- физические лица, состоящие с учреждением в гражданско-правовых отношениях;
- физические лица, обратившиеся в учреждение за платными медицинскими услугами.

4.2.4. Данные, обрабатываемые Организацией:

- данные, полученные при осуществлении трудовых отношений;
- данные, полученные для осуществления отбора кандидатов на работу в Организацию;
- данные, полученные при осуществлении гражданско-правовых отношений;
- данные, полученные при оказании платных медицинских услуг.

Полный список Данных представлен в Перечне Данных, утвержденном главным врачом Организации.

4.2.5. Обработка персональных данных ведется:

- с использованием средств автоматизации;
- без использования средств автоматизации.

4.3. Хранение Данных.

4.3.1. Данные субъектов могут быть получены, проходить дальнейшую обработку и передаваться на хранение как на бумажных носителях, так и в электронном виде.

4.3.2. Данные, зафиксированные на бумажных носителях, хранятся в запираемых шкафах либо в запираемых помещениях с ограниченным правом доступа (регистратура).

4.3.3. Данные субъектов, обрабатываемые с использованием средств автоматизации в разных целях, хранятся в разных папках (вкладках).

4.3.4. Не допускается хранение и размещение документов, содержащих Данные, в открытых электронных каталогах (файлообменниках) в ИСПД.

4.3.5. Хранение Данных в форме, позволяющей определить субъекта Данных, осуществляется не дольше, чем этого требуют цели их обработки, и они подлежат уничтожению по достижении целей обработки или в случае утраты необходимости в их достижении.

4.4. Уничтожение Данных.

4.4.1. Уничтожение документов (носителей), содержащих Данные, производится путем сожжения, дробления (измельчения), химического разложения, превращения в бесформенную массу или порошок. Для уничтожения бумажных документов допускается применение шредера.

4.4.2. Данные на электронных носителях уничтожаются путем стирания или форматирования носителя.

4.4.3. Уничтожение производится комиссией. Факт уничтожения Данные подтверждается документально актом об уничтожении носителей, подписанными членами комиссии.

4.5. Передача Данных.

4.5.1 Организация передает Данные третьим лицам в следующих случаях:

- субъект выразил свое согласие на такие действия;
- передача предусмотрена российским или иным применимым законодательством в рамках установленной законодательством процедуры.

4.5.2 Перечень лиц, которым передаются Данные:

Третьи лица, которым передаются Данные:

- Пенсионный фонд РФ для учета (на законных основаниях);
- Налоговые органы РФ (на законных основаниях);
- Фонд социального страхования (на законных основаниях);
- банки для начисления заработной платы (на основании договора);
- судебные и правоохранительные органы в случаях, установленных законодательством;

5. Защита персональных данных

5.1. В соответствии с требованиями нормативных документов Организацией создана система защиты персональных данных (СЗПД), состоящая из подсистем правовой, организационной и технической защиты.

5.2 Подсистема правовой защиты представляет собой комплекс правовых, организационно-распорядительных и нормативных документов, обеспечивающих создание, функционирование и совершенствование СЗПД.

5.3 Подсистема организационной защиты включает в себя организацию структуры управления СЗПД, защиты информации при работе с сотрудниками, партнерами и сторонними лицами, защиты информации в открытой печати, публикаторской и рекламной деятельности, аналитической работы.

5.4 Подсистема технической защиты включает в себя комплекс технических, программных, программно-аппаратных средств, обеспечивающих защиту Данных

5.5 Основными мерами защиты Данных, используемыми Организацией, являются:

- назначение лица, ответственного за обработку Данных, которое осуществляет организацию обработки Данных, обучение и инструктаж, внутренний контроль за соблюдением учреждением и его работниками требований к защите Данных;
- определение актуальных угроз безопасности Данных при их обработке в ИСПД, и разработка мер и мероприятий по защите Данных;
- разработка политики в отношении обработки персональных данных;
- установление правил доступа к Данным, обрабатываемым в ИСПД, а также обеспечения регистрации и учета всех действий, совершаемых с Данными в ИСПД;
- установление индивидуальных паролей доступа сотрудников в информационную систему в соответствии с их производственными обязанностями;
- применение средств защиты информации, учет машинных носителей Данных, обеспечение их сохранности;
- сертифицированное программное средство защиты информации от несанкционированного доступа;
- сертифицированные межсетевой экран и средство обнаружения вторжения;
- соблюдение условий, обеспечивающих сохранность Данных и исключающие несанкционированный к ним доступ, оценка эффективности принимаемых и реализованный к ним доступ, оценка эффективности принимаемых и реализованных мер по обеспечению безопасности Данных;
- установление правил доступа к обрабатываемым Данным, обеспечение регистрации и учета действий, совершаемых с Данными, а также обнаружение фактов несанкционированного доступа к персональным данным и принятия мер;
- восстановление Данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
- обучение работников Организации, непосредственно осуществляющих обработку персональных данных, положениям законодательства Российской Федерации о персональных данных, в том числе требованиям к защите персональных данных, документам, определяющим политику Организации в отношении обработки персональных данных, локальных актам по вопросам обработки персональных данных;
- осуществление внутреннего контроля и аудита.

6. Основные права субъекта Данных и обязанности Организации

6.1. Субъект Данных имеет право на получении информации, касающейся обработки его персональных данных, в том числе содержащей:

- подтверждение факта обработки персональных данных оператором;
- правовые основания и цели обработки персональных данных;
- цели и применяемые оператором способы обработки персональных данных;

- наименование и место нахождения оператора, сведения о лицах (за исключением работников оператора), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с оператором или на основании федерального закона;
- обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;
- сроки обработки персональных данных, в том числе сроки их хранения;
- порядок осуществления субъектом персональных данных прав, предусмотренных Федеральным законом «О персональных данных»;
- информацию об осуществленной или о предполагаемой трансграничной передаче данных;
- наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению оператора, если обработка поручена или будет поручена такому лицу; иные сведения, предусмотренные настоящим Федеральным законом или другими федеральными законами.

Субъект Данных вправе 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.

6.2. Организация обязана:
- при сборе предоставить информацию об обработке его Данных;
- в случаях если Данные были получены не от субъекта Данных уведомить субъекта;
- при отказе в предоставлении Данных субъекту разъясняются последствия такого отказа;
- опубликовать или иным образом обеспечить неограниченный доступ к документу, определяющему его политику в отношении обработки Данных, к сведениям о реализуемых требованиях к защите Данных;
- принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие для защиты Данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения Данных, а также от иных неправомерных действий в отношении Данных;
- давать ответы на запросы и обращения субъектов Данных, их представителей и уполномоченного органа по защите прав субъектов Данных.