# Политика обработки персональных данных и реализуемых требований к защите персональных данных

# ООО «МЕДСКАН»

## 1. Общие положения

1.1. Настоящая Политика разработана в соответствии с положениями Конституции РФ от 12.12.1993г (ст.ст. 2, 17-24, 41), Трудового кодекса РФ, Федерального закона от 27.07. 2006 № 152-ФЗ "О персональных данных", Федерального закона от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и защите информации», Постановлением Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», Постановлением Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», Федерального закона Российской Федерации от 21.11.2011 № 323-ФЗ "Об основах охраны здоровья граждан в Российской Федерации", Федерального закона Российской Федерации от 29.11.2010 №326-ФЗ «Об обязательном медицинском страховании в Российской Федерации» и иных нормативно-правовых актов, регулирующих вопросы защиты персональных данных.
1.2. Настоящая Политика определяет основные вопросы, связанные с обработкой персональных данных в ООО «МЕДСКАН» (далее - Оператор) с использованием средств автоматизации, в том числе в информационно-телекоммуникационных сетях, или без использования таких средств.
1.3. Персональные данные являются конфиденциальной, охраняемой информацией и на них распространяются все требования, установленные внутренними документами Оператора к защите конфиденциальной информации.

## 2. Термины и состав персональных данных

**2.1. Оператор** – юридическое 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;
**2.2. 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;
**2.3. Субъект персональных данных** – заказчики услуг Оператора и пациенты Оператора – физические лица, в том числе потенциальные заказчики и пациенты, представители заказчиков и пациентов, пользователи Корпоративного сайта Оператора.
**2.4. Врачебная тайна** – сведения о факте обращения пациента за оказанием медицинской помощи, состоянии его здоровья и диагнозе, иные сведения, полученные при его медицинском обследовании и лечении.
**2.5. Персональные данные (ПД)** – любая информация, в том числе, если применимо, составляющая врачебную тайну, относящаяся к прямо или косвенно определенному или определяемому субъекту персональных данных.
2.6. Оператор обрабатывает персональные данные следующих категорий субъектов персональных данных:

- персональные данные работников Оператора - информация, необходимая Оператору в связи с трудовыми отношениями;

- персональные данные пациента, заказчика, клиента (потенциального клиента), партнера, контрагента (потенциального контрагента), а также персональные данные руководителя, участника (акционера) или сотрудника юридического лица, являющегося клиентом или контрагентом (потенциальным клиентом, партнером, контрагентом) Оператора - информация, необходимая Оператору для выполнения своих обязательств в рамках договорных отношений с пациентом,клиентом (контрагентом);

**3. Цели и случаи обработки персональных данных**

3.1. Целями обработки персональных данных являются:

- организация кадрового учета, ведение кадрового делопроизводства, содействие работникам в трудоустройстве, обучении и продвижении по службе, исполнение налогового законодательства РФ в связи с исчислением и уплатой НДФЛ, а также пенсионного законодательства РФ при формировании и представлении персонифицированных данных о каждом получателе доходов, учитываемых при начислении страховых взносов на обязательное пенсионное страхование и обеспечение, заполнение первичной статистической документации;
- заключение, исполнение и прекращение гражданско-правовых договоров;
- закрепление принципов защиты персональных данных субъектов персональных данных Оператора, обеспечение их прав и свобод, установление правил обработки персональных данных и их защиты.

3.2. Обработка персональных данных Оператором допускается в случаях:

- если обработка персональных данных осуществляется с согласия субъекта персональных данных;

- если обработка персональных данных необходима для исполнения договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных, а также для заключения договора по инициативе субъекта персональных данных или договора, по которому субъект персональных данных будет являться выгодоприобретателем или поручителем;

- если обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных, если получение согласия субъекта персональных данных невозможно;

- если обработка персональных данных необходима для осуществления прав и законных интересов Оператора или третьих лиц либо для достижения общественно значимых целей при условии, что при этом не нарушаются права и свободы субъекта персональных данных;

- если обработка персональных данных необходима для осуществления научной, литературной или иной творческой деятельности при условии, что при этом не нарушаются права и законные интересы субъекта персональных данных;

- если обработка персональных данных осуществляется в исследовательских, статистических или иных целях при условии обязательного обезличивания персональных данных;
- если осуществляется обработка персональных данных, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных либо по его просьбе;
- если осуществляется обработка персональных данных, подлежащих опубликованию или обязательному раскрытию в соответствии с законом;

3.3. Обработка персональных данных в ООО «МЕДСКАН » осуществляется в следующих целях:

- для целей заключения и исполнения договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных

данных, обработка персональных данных осуществляется на основании Федерального закона от 27.07. 2006 № 152-ФЗ "О персональных данных".

- в медико-профилактических целях, в целях установления медицинского диагноза, оказания медицинских и медико-социальных услуг при условии, что обработка персональных данных осуществляется лицом, профессионально занимающимся медицинской деятельностью и обязанным в соответствии с законодательством Российской Федерации сохранять врачебную тайну, обработка персональных данных осуществляется на основании Федерального закона от 27.07. 2006 № 152-ФЗ "О персональных данных".

- для целей предоставления Оператором дополнительных сервисов субъектам персональных данных, упрощения порядка взаимодействия между Оператором и субъектами персональных данных, для исполнения требований правил оказания платных медицинских услуг и проверки качества оказания услуг заказчиком, обработка персональных данных осуществляется на основании письменного согласия субъекта персональных данных.

- для иных целей обработка персональных данных осуществляется на основании согласия субъекта персональных данных при условии получения согласия на конкретные цели обработки персональных данных.

3.4. В отдельных случаях, Оператор вправе осуществлять обработку персональных данных субъекта персональных данных без получения его согласия, если такие действия необходимы для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных.

3.5. Персональные данные специальной категории обрабатываются Оператором только при наличии согласия субъекта в письменной форме.

3.6. Оператор не осуществляет обработку иных персональных данных, которые не отвечают целям такой обработки, а также законным правам и интересам субъекта персональных данных.

3.7. Оператор самостоятельно и за свой счет обеспечивает организационно-технические мероприятия, а также принимает меры по обеспечению защиты персональных данных субъектов персональных данных.

**4. Основные принципы обработки персональных данных**

4.1. Обработка персональных данных возможна только в соответствии с целями, определившими их получение.

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

4.3. Право доступа для обработки персональных данных имеют сотрудники Оператора в соответствии с возложенными на них функциональными обязанностями.

4.4. При обработке персональных данных обеспечивается точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к заявленным целям их обработки.

4.5. Хранение персональных данных осуществляется 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.

4.6. Обрабатываемые персональные данные уничтожаются или обезличиваются по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

4.7. Сроки хранения персональных данных определяются в соответствии со сроком действия гражданско-правовых отношений между субъектом персональных данных и Оператором, сроком исковой давности, сроками хранения документов на бумажных носителях и документов в электронных базах данных, иными требованиями

законодательства РФ, а также сроком действия согласия субъекта на обработку его персональных данных.
4.8. Оператор осуществляет обработку персональных данных субъектов персональных данных 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 Оператора;
- 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;

**5. Порядок получения персональных данных субъекта персональных данных**
5.1. Субъект персональных данных предоставляет персональные данные, а Оператор осуществляет их дальнейшую обработку на основании письменного согласия за исключением случаев предусмотренных законодательством.
5.2. Оператор гарантирует, что субъект персональных данных принимает решение о предоставлении его персональных данных и дает согласие на их обработку свободно, по своей волей и в своем интересе. Обязанность предоставить доказательство получения согласия субъекта персональных данных на обработку его персональных данных или доказательство наличия оснований, указанных в Федеральном законе от 27.07.2006 № 152-ФЗ «О персональных данных», возлагается на Оператора.
5.3. Письменное согласие:
5.3.1. Согласие на обработку персональных данных должно быть конкретным, информированным и сознательным.
5.3.2. Форма письменного согласия на обработку персональных данных определяется Оператором, и утверждается руководителем Оператора.
5.3.3. Форма письменного согласия в обязательном порядке включает в себя следующее:
- фамилию, имя, отчество, адрес субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;
- фамилию, имя, отчество, адрес представителя субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе, реквизиты доверенности или иного документа, подтверждающего полномочия этого представителя (при получении согласия от представителя субъекта персональных данных);
- наименование, реквизиты и адрес Оператора, получающего согласие субъекта персональных данных;
- цель обработки персональных данных;
- перечень персональных данных, на обработку которых дается согласие субъекта персональных данных;
- перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых оператором способов обработки персональных данных;
- срок, в течение которого действует согласие субъекта персональных данных, а также способ его отзыва, если иное не установлено федеральным законом;
- подпись субъекта персональных данных.
5.3.4. Равнозначным содержащему собственноручную подпись субъекта персональных данных согласию в письменной форме на бумажном носителе является согласие в форме электронного документа, подписанного в соответствии с федеральным законом электронной подписью.

5.3.5. В случае смерти субъекта персональных данных согласие на обработку его персональных данных дают наследники субъекта персональных данных, если такое согласие не было дано субъектом персональных данных при его жизни.

**6. Обработка персональных данных**

6.1. Порядок обработки персональных данных субъектов определяется должностными инструкциями Оператора, приказами и иными локальными нормативными актами.

6.2. Обработка Оператором персональных данных субъектов персональных данных осуществляется автоматизированным и неавтоматизированным способами (смешанный тип).

6.3. Обработка персональных данных – общие положения:

6.3.1. Правом обработки персональных данных субъекта наделяются работники Оператора, допущенные к работе с теми или иными персональными данными, а также третьи лица, которые имеют доступ к персональным данным субъекта в силу договорных отношений с Оператором при условии соблюдения условия о конфиденциальности персональных данных.

6.3.2. Работнику Оператора предоставляется право использовать только те персональные данные, использование которых необходимо для реализации, закрепленной за ним трудовой функции, и возложенных на него трудовых обязанностей.

6.3.3. Перечень лиц, имеющих доступ к тем или иным персональным данным, устанавливается руководителем Оператора, путем подписания соответствующего приказа, если иное не вытекает из другого локального нормативного акта, утвержденного Оператором в установленном порядке.

6.4. Хранение носителей персональных данных:

6.4.1. Хранение носителей персональных данных осуществляется в соответствии с условиями настоящей Политики, должностных инструкций и иных локальных нормативных актов, утвержденных Оператором.

6.4.2. Хранение бумажных носителей персональных данных (медицинские карты, распечатки и иные документы), а также цифровых носителей (жесткие диски, CD, флеш-карты и др.) осуществляется в специально предназначенных для этого шкафах или иных местах хранения, расположенных в помещениях, оборудованных электронной системой разграничения допуска.

6.4.3. Шкафы, в которых хранятся персональные данные, оборудованы замками, и, при необходимости, иными средствами, ограничивающими доступ к ним.

6.4.4. Доступ к таким помещениям, в которых хранятся шкафы, содержащие носители персональных данных субъектов персональных данных, имеют лишь уполномоченные сотрудники.

6.4.5. В случае возникновения необходимости доступа в такое помещение лицом, доступ которого к персональным данным должен быть ограничен (уборка, ремонтные работы и др.), необходимо обеспечить достаточные меры, которые позволят не допустить реализации актуальных угроз персональных данных.

**7. Меры по обеспечению безопасности персональных данных**

7.1. Защита персональных данных – комплекс мер, направленных на:

- обеспечение режима конфиденциальности информации в отношении персональных данных, сохранение врачебной тайны;
- защиту персональных данных от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий;
- обеспечение законных прав и интересов субъектов персональных данных.

7.2. Защита персональных данных субъектов персональных данных осуществляется силами всех сотрудников Оператора на основании комплекса утвержденных документов и мер, регламентирующих правила обработки персональных данных, а также может осуществляться путем привлечения специализированных организаций.
7.3. Защита персональных данных в информационных системах персональных данных, используемых Оператором, осуществляется в соответствии с данной Политикой, Положением об обработке и защите персональных данных в информационных системах персональных данных, должностными инструкциями и иными локальными нормативными актами, принятыми Оператором.
7.4. Обеспечение безопасности персональных данных достигается, в частности:
- применением организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные Правительством РФ уровни защищенности персональных данных;
- обнаружением фактов несанкционированного доступа к персональным данным и принятием необходимых мер;
- установлением правил доступа к персональным данным, обрабатываемым в информационной системе персональных данных, а также обеспечением регистрации и учета всех действий, совершаемых с персональными данными в информационной системе персональных данных;
- контролем за принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности информационной системы персональных данных.

**8. Права субъекта персональных данных**
8.1. Субъект персональных данных имеет право на получение 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 такие данные на основании договора с Оператором или на основании законодательства;
- обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен законодательством;
- сроки обработки персональных данных, в том числе сроки их хранения;
- порядок осуществления субъектом персональных данных прав, предусмотренных действующим законодательством;
- информацию об осуществленной или о предполагаемой трансграничной передаче персональных данных;
- наименование или фамилию, имя, отчество и адрес лиц, осуществляющих обработку персональных данных по поручению Оператора, если обработка поручена или будет поручена таким лицам;
- иные сведения, предусмотренные законодательством РФ;
8.2. Сведения, указанные в п. 8.1. настоящей Политики, должны быть предоставлены субъектам персональных данных Оператором в доступной форме, и в них не должны содержаться персональные данные, относящиеся к другим субъектам персональных данных, за исключением случаев, если имеются законные основания для раскрытия таких персональных данных.

8.3. Сведения, указанные п. 8.1. настоящей Политики, предоставляются субъекту персональных данных или его представителю Оператором при обращении либо при получении Запроса субъекта персональных данных или его представителя в течение 30 (тридцати) календарных дней с момента получения соответствующего запроса Оператором.
8.4. Запрос, указанный в п. 8.3. настоящей Политики, должен содержать номер основного документа, удостоверяющего личность субъекта персональных данных или его представителя, сведения о дате выдачи указанного документа и выдавшем его органе, сведения, подтверждающие участие субъекта персональных данных в отношениях с Оператором (номер договора, дата заключения договора, номер амбулаторной карты и др.), либо сведения, иным образом подтверждающие факт обработки персональных данных Оператором, подпись субъекта персональных данных или его представителя. Запрос может быть направлен в форме электронного документа и подписан электронной подписью в соответствии с законодательством Российской Федерации.
8.5. Субъект персональных данных вправе требовать от Оператора уточнения его персональных данных, их блокирования или уничтожения в случае, если такие 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.
8.6. На свободный бесплатный доступ к своим персональным данным, включая право на получение копий любой записи, содержащей персональные данные, за исключением случаев, предусмотренных законодательством РФ.
8.7. В отдельных случаях, предусмотренных законодательством, право субъекта персональных данных на доступ к его персональным данным может быть ограничено.
8.8. Если субъект персональных данных считает, что Оператор осуществляет обработку его персональных данных с нарушением требований законодательства или иным образом нарушает его права и свободы, субъект персональных данных вправе обжаловать действия или бездействие Оператора в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке.
8.9. Субъект персональных данных имеет право на защиту своих прав и законных интересов, в том числе на возмещение убытков и (или) компенсацию морального вреда в судебном порядке.

**9. Обязанности оператора**

Оператор обязуется:
9.1. Принимать необходимые и достаточные правовые, организационные и технические меры для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.
9.2. Осуществлять мероприятия по организационной и технической защите персональных данных в соответствии с требованиями законодательства РФ по вопросам обработки персональных данных.
9.3. В целях обеспечения защиты персональных данных проводить оценку вреда, который может быть причинен субъектам персональных данных в случае нарушения безопасности их персональных данных, а также определять актуальные угрозы безопасности персональных данных при их обработке в информационных системах персональных данных.
9.4. При выявлении актуальных угроз применять необходимые и достаточные правовые, организационные и технические меры по обеспечению безопасности персональных данных, включающие в себя:
- определение угроз безопасности информации, содержащей персональные данные, при ее обработке;

- применение организационных и технических мер по обеспечению безопасности информации, содержащей персональные данные, при ее обработке;
- оценку эффективности принимаемых мер до ввода в эксплуатацию информационной системы персональных данных;
- учет машинных носителей информации, содержащей персональные данные;
- обнаружение фактов несанкционированного доступа к информации, содержащей персональные данные, и принятие мер;
- восстановление персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
- установление правил доступа к информации, содержащей персональные данные, обеспечение регистрации и учета всех действий, совершаемых с информацией, содержащей персональные данные, в информационной системе персональных данных;
- контроль за принимаемыми мерами.

**10. Обязанности и ответственность сотрудников оператора**

10.1. Сотрудники Оператора, допущенные к обработке персональных данных, обязаны:
- знать и неукоснительно выполнять требования настоящей Политики;
- обрабатывать персональные данные только в рамках выполнения своих должностных обязанностей;
- не разглашать персональные данные, полученные в результате выполнения своих должностных обязанностей, а также ставшие им известными по роду своей деятельности;
- пресекать действия третьих лиц, которые могут привести к разглашению (уничтожению, искажению) персональных данных;
- выявлять факты разглашения (уничтожения, искажения) персональных данных и информировать об этом непосредственного руководителя;
- хранить тайну о сведениях, содержащих персональные данные в соответствии с локальными актами Оператора.

10.2. Сотрудникам Оператора, допущенным к обработке персональных данных, запрещается несанкционированное и нерегламентированное копирование персональных данных на бумажные носители информации и на любые электронные носители информации, не предназначенные для хранения персональных данных.

10.3. Каждый новый работник Оператора, непосредственно осуществляющий обработку персональных данных, подлежит ознакомлению с требованиями законодательства РФ по обработке и обеспечению безопасности персональных данных, с настоящей Политикой и другими локальными актами по вопросам обработки и обеспечения безопасности персональных данных и обязуется их соблюдать.

10.4. Лица, виновные в нарушении требований законодательства РФ в области персональных данных, несут дисциплинарную, материальную, гражданско-правовую, административную или уголовную ответственность.

**11. Заключительные положения**

11.1. Действующая редакция Политики на бумажном носителе хранится в медицинском центре ООО «МЕДСКАН» по адресу: г. Москва, Ленинградское ш. 47А

11.2. Электронная версия действующей редакции Политики общедоступна на сайте Оператора в сети Интернет [**medscannet.ru**].

11.3. При внесении изменений в заголовке Политики указывается дата утверждения действующей редакции Политики.

11.4. Политика актуализируется и заново утверждается на регулярной основе - ежегодно.

11.5. Политика может актуализироваться и заново утверждаться ранее срока, указанного в п. 11.4. настоящей Политики, по мере внесения изменений в нормативные правовые акты в сфере персональных данных или в локальные акты, регламентирующие организацию обработки и обеспечение безопасности персональных данных.