Утверждаю Генеральный директор
ООО «Медицинская компания
«Эстет»
Нашунькин А.Г. Приказ № 02-01/25
от «03» января 2025 года

ПОЛИТИКА
в области обработки и обеспечения безопасности персональных данных в ООО «Медицинская компания «Эстет»

1. Общие положения

1.1. Настоящая Политика в области обработки и обеспечения безопасности персональных данных (далее - Политика) составлена в соответствии с п. 2 ст. 18.1 Федерального закона РФ «О персональных данных» № 152-ФЗ от 27 июля 2006 года и действует в отношении всех персональных данных, которые ООО «Медицинская компания «Эстет» (далее - Оператор) может получить от субъекта персональных данных, являющегося стороной по договору оказания медицинских услуг с Оператором (далее – Получатель/Пациент), или от субъекта персональных данных, состоящего с Оператором в отношениях, регулируемых трудовым законодательством (далее - Работника). Политика распространяется на персональные данные полученные как до, так и после подписания настоящей Политики.

1.2. Целью Политики является определение правильного способа обработки персональных данных, а также разработка на его основе процедур, предотвращающих или реагирующих на нарушение безопасности персональных данных.

1.3. К настоящей Политике имеет доступ любой субъект персональных данных.

1.4. Основные понятия, используемые в Политике:

персональные данные - любая информация, относящаяся к прямо или косвенно определенному, или определяемому физическому лицу (субъекту персональных данных);

оператор персональных данных (Оператор) - общество с ограниченной ответственностью «Медицинская компания «Эстет», осуществляющее обработку персональных данных, а также определяющий цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными;

обработка персональных данных - любое действие (операция) или совокупность действий (операций) с персональными данными, совершаемых с использованием средств автоматизации или без их использования. Обработка персональных данных включает в себя, в том числе: сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение;

автоматизированная обработка персональных данных - обработка персональных данных с помощью средств вычислительной техники;

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;
информационная система персональных данных - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств;
трансграничная передача персональных данных - передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу;

субъект персональных данных - физическое лицо, которое прямо или косвенно определено с помощью персональных данных.

1.5. Основные права и обязанности Субъекта персональных данных и Оператора:
1.5.1. Субъект персональных данных имеет право на свободный доступ к своим персональным данным, включая право на получение копии любой записи (за исключением случаев, предусмотренных законодательством), содержащей его персональные данные.
1.5.2. Субъект персональных данных имеет право на получение от Оператора информации, содержащей:
- подтверждения факта обработки персональных данных Оператором;
- правовых оснований и целей обработки персональных данных;
- целей и применяемых Оператором способов обработки персональных данных;
- наименования и места нахождения Оператора, сведений 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;
- обрабатываемых персональных данных, относящихся к соответствующему субъекту персональных данных, источника их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;
- сроков обработки персональных данных, в том числе сроков их хранения;
- порядка осуществления субъектом персональных данных прав, предусмотренных Федеральным законом № 152-ФЗ;
- иных сведений, предусмотренных действующим законодательством.
1.5.3. Субъект персональных данных вправе отозвать свое согласие на обработку персональных данных, если иное не предусмотрено условиями договора с субъектом персональных данных или Федеральным законом № 152-ФЗ.
1.5.4. Субъект персональных 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.
1.5.5. Для реализации вышеуказанных прав субъекту персональных данных необходимо направить в адрес Оператора соответствующее письменное обращение. Если иное не предусмотрено договором между Оператором и субъектом персональных данных или в согласии на обработку персональных данных, обращение направляется Оператору одним из следующих способов:
в произвольной форме на бумажном носителе по адресу Оператора;
- лично обратиться с письменным заявлением в Организацию Оператора.
1.5.6. Субъект персональных данных вправе обжаловать действия или бездействие Оператора в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке, если считает, что Оператор осуществляет обработку его персональных данных с нарушением требований Федерального закона № 152-ФЗ или иным образом нарушает его права и свободы.
1.5.7. 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.
1.5.8. Оператор обязан:
- при сборе персональных данных предоставить субъекту персональных данных по его

просьбе информацию, указанную в п. 1.5.2 настоящей Политики;
- разъяснить субъекту персональных данных юридические последствия отказа предоставить его персональные данные, если предоставление персональных данных является обязательным в соответствии с федеральным законом;
- в порядке, предусмотренном Федеральным законом № 152-ФЗ, сообщить субъекту персональных данных или его представителю информацию о наличии персональных данных, относящихся к соответствующему субъекту персональных данных, а также предоставить возможность ознакомления с этими персональными данными при обращении субъекта персональных данных или его представителя либо в течение тридцати дней с даты получения запроса субъекта персональных данных или его представителя;
- в случае отказа в предоставлении информации о наличии персональных данных о соответствующем субъекте персональных данных или персональных данных субъекту персональных данных или его представителю при их обращении либо при получении запроса субъекта персональных данных или его представителя дать в письменной форме мотивированный ответ, содержащий ссылку на положение федерального закона, являющееся основанием для такого отказа, в срок, не превышающий тридцати дней со дня обращения субъекта персональных данных или его представителя либо с даты получения запроса субъекта персональных данных или его представителя;
- принимать меры, необходимые и достаточные для обеспечения выполнения обязанностей, предусмотренных Федеральным законом № 152-ФЗ и принятыми в соответствии с ним нормативными правовыми актами;
- в случаях, предусмотренных Федеральным законом № 152-ФЗ немедленно прекратить по требованию субъекта персональных данных обработку его персональных данных;

при обработке персональных данных принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие 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;
- исполнять иные требования законодательства в области защиты персональных данных.

2. Цели сбора персональных данных

2.1. Цели сбора персональных данных

- обеспечение организации оказания медицинской помощи населению, а также наиболее полного исполнения обязательств и компетенций в соответствии с законами от 21 ноября 2011 г. № 323-ФЗ «Об основах охраны здоровья граждан Российской Федерации», от 12 апреля 2010 г. № 61-ФЗ «Об обращении лекарственных средств», Правилами предоставления медицинскими организациями платных медицинских услуг, утвержденными постановлением Правительства РФ от 11 мая 2023 г. № 736;
- ведения кадрового делопроизводства и организации учета работников Оператора, в том числе привлечения и отбора кандидатов на работу у Оператора, обучения, добровольного страхования всех видов, продвижения по службе, предоставления работникам различного вида льгот и компенсаций;
- осуществление гражданско-правовых отношений.

3. Правовые основания обработки персональных данных

3.1. Правовым основанием обработки персональных данных является совокупность правовых актов, во исполнение которых и в соответствии с которыми Оператор осуществляет обработку персональных данных.

3.2. Правовыми основаниями обработки персональных данных являются:
. Конституция Российской Федерации;
. Гражданский кодекс Российской Федерации;
. Трудовой кодекс Российской Федерации;
. Налоговый кодекс Российской Федерации;
- Федеральный закон от 21 ноября 2011 г. № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации»
- Федеральный закон от 01.04.1996 № 27-ФЗ «Об индивидуальном (персонифицированном) учете в системе обязательного пенсионного страхования»;

- Федеральный закон от 02.12.1990 № 395-1 «О банках и банковской деятельности»;
- Федеральный закон от 08.02.1998 № 14-ФЗ «Об обществах с ограниченной ответственностью»;
- Федеральный закон от 06.12.2011 № 402-ФЗ «О бухгалтерском учете»;
- иные федеральные законы и принятые на их основе нормативные правовые акты, регулирующие отношения, связанные с деятельностью Оператора;
- Указ Президента Российской Федерации от 06 марта 1997 г. № 188 «Об утверждении Перечня сведений конфиденциального характера»;
- Постановление Правительства Российской Федерации от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;
- Постановление Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- Приказ ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;
- Приказ Роскомнадзора от 05 сентября 2013 г. № 996 «Об утверждении требований и методов по обезличиванию персональных данных»; иные нормативные правовые акты Российской Федерации и нормативные документы уполномоченных органов государственной власти.
- договоры, заключаемые между Оператором и субъектом персональных данных;
- договоры, заключаемые Оператором с контрагентами;
- Устав Оператора и иные внутренние документы Оператора;
- согласие на обработку персональных данных (в случаях, прямо непредусмотренных законодательством Российской Федерации, но соответствующих полномочиям Оператора).

4. Объем и категории обрабатываемых персональных данных, категории субъектов персональных данных

4.1. Оператор осуществляет обработку персональных данных следующих категорий субъектов персональных данных;
- работников Оператора, в том числе бывших работников;
- физических лиц, являющих кандидатами на должность;
- клиентов (пациентов) и их представителей;
- контрагентов Оператора (физических лиц), заключивших или намеревающихся заключить с Оператором гражданско-правовые договоры;
- представителей/работников корпоративных клиентов и контрагентов Оператора, заключивших или намеревающихся заключить договор с Оператором;
- физических лиц, входящих в органы управления Оператора, и их близких родственников;
- иных физических лиц, выразивших согласие на обработку Оператором их персональных данных или физических лиц, обработка персональных данных которых необходима Оператору для достижения целей, предусмотренных международным договором Российской Федерации или законом, для осуществления и выполнения возложенных законодательством Российской Федерации на Оператора функций, полномочий и обязанностей.

4.1. Персональные данные, обрабатываемые Оператором:

4.1.1. Персональные данные физических лиц (пациентов):

1) фамилия, имя, отчество (последнее - при наличии);
2) пол;
3) дата рождения;
4) место рождения;
5) гражданство;
6) данные документа, удостоверяющего личность;
7) место жительства;
8) место регистрации;
9) дата регистрации;

10) страховой номер индивидуального лицевого счета (при наличии), принятый в соответствии с законодательством Российской Федерации об индивидуальном (персонифицированном) учете в системе обязательного пенсионного страхования;
11) анамнез;
12) диагноз;
13) сведения об организации, оказавшей медицинские услуги;
14) вид оказанной медицинской помощи;
15) условия оказания медицинской помощи;
16) сроки оказания медицинской помощи;
17) объем оказанной медицинской помощи;
18) результат обращения за медицинской помощью;
19) серия и номер выданного листка нетрудоспособности (при наличии);
20) сведения об оказанных медицинских услугах;
21) примененные стандарты медицинской помощи;
22) сведения о медицинском работнике или медицинских работниках, оказавших медицинскую услугу.
23) иная информация, необходимая для правильного и качественного оказания медицинских услуг и ведения медицинского учета.
4.1.2. Персональные сотрудников Оператора (кандидатов, бывших сотрудников):
1. Фамилия, имя, отчество;
2. Место, год и дата рождения;
3. Адрес по прописке;
4. Паспортные данные (серия, номер паспорта, кем и когда выдан);
5. Информация об образовании (наименование образовательного учреждения, сведения о документах, подтверждающие образование: наименование, номер, дата выдачи, специальность);
7. Информация о трудовой деятельности до приема на работу;
8. Информация о трудовом стаже (место работы, должность, период работы, период работы, причины увольнения);
9. Адрес проживания (реальный);
10. Телефонный номер (домашний, рабочий, мобильный);
11. Семейное положение и состав семьи (муж/жена, дети);
12. Информация о знании иностранных языков;
13. Форма допуска;
14. Оклад;
15 Данные о трудовом договоре (№ трудового договора, дата его заключения, дата начала и дата окончания договора, вид работы, срок действия договора, наличие испытательного срока, режим труда, длительность основного отпуска, длительность дополнительного отпуска, длительность дополнительного отпуска за ненормированный рабочий день, обязанности работника, дополнительные социальные льготы и гарантии, № и число изменения к трудовому договору, характер работы, форма оплаты, категория персонала, условия труда, продолжительность рабочей недели, система оплаты);
16 Сведения о воинском учете (категория запаса, воинское звание, категория годности к военной службе, информация о снятии с воинского учета);
17. ИНН;
18. Данные об аттестации работников;
19. Данные о повышении квалификации;
20. Данные о наградах, медалях, поощрениях, почетных званиях;
21. Информация о приеме на работу, перемещении по должности, увольнении;
22. Информация об отпусках;
23. Информация о командировках;
24. Информация о негосударственном пенсионном обеспечении.

5. Порядок и условия обработки персональных данных

5.1. Обработка персональных данных осуществляется Оператором в соответствии с требованиями законодательства Российской Федерации.
5.2. Обработка персональных данных осуществляется в порядке, исключающем неправомерный или случайный доступ к персональным данным, в том числе третьих лиц.

5.3. Перечень действий, совершаемых Оператором с персональными данными: сбор, запись, систематизация, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передача (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение.
5.4. При сборе персональных данных, в том числе посредством информационно-телекоммуникационной сети "Интернет", Оператор обеспечивает запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение персональных данных граждан Российской Федерации с использованием баз данных, находящихся на территории Российской Федерации, за исключением случаев, указанных в Федеральным законом № 152-ФЗ.
5.5. Оператор осуществляет как автоматизированную, так и неавтоматизированную обработку персональных данных. Оператор не принимает на основании исключительно автоматизированной обработки персональных данных решений, порождающих юридические последствия в отношении субъекта персональных данных, или иным образом затрагивающих его права и законные интересы, кроме случаев и условий, предусмотренных законодательством Российской Федерации.
5.6. Обработка персональных данных осуществляется с согласия субъекта персональных данных на обработку персональных данных, а также без такового, в случаях, предусмотренных действующим законодательством РФ.
5.7. Доступ к персональным данным предоставляется только тем работникам Оператора, которым он необходим в связи с исполнением ими своих должностных обязанностей и с соблюдением принципов персональной ответственности. Процедура оформления доступа к персональным данным включает в себя ознакомление работника с внутренними документами Оператора, регламентирующими процесс обработки и защиты персональных данных, а также получение письменного обязательства работника о неразглашении персональных данных. При увольнении работника, имеющего доступ к персональным данным, документы и иные носители, содержащие персональные данные, передаются его непосредственному руководителю, а доступ работника к информационным системам персональных данных отзывается.
5.8. Оператор не раскрывает третьим лицам и не распространяет персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом. Оператор вправе передавать персональные данные органам дознания и следствия, иным уполномоченным органам по основаниям, предусмотренным действующим законодательством Российской Федерации.
5.9. Оператор вправе поручить обработку персональных данных другому лицу с согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.
5.10. Оператор осуществляет хранение персональных данных 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.
5.11. Документы на бумажных носителях, содержащие персональные данные субъектов, хранятся в специализированных помещениях, шкафах или сейфах.
5.12. Персональные данные субъектов также хранятся с использованием средств автоматизации в информационных системах Оператора. Ограничение доступа к информационным системам, содержащим персональные данные субъектов, обеспечивает Система защиты персональных данных Оператора - совокупность организационных мер и технических средств защиты информации, а также используемых в информационной системе информационных технологий, в рамках которых реализуются организационные и технические мероприятия, обеспечивающие безопасность обрабатываемых персональных данных.
5.13. Срок хранения персональных данных устанавливается в соответствии с действующим законодательством в зависимости от состава персональных данных.

6. Актуализация, исправление, удаление и уничтожение персональных данных, ответы на запросы субъектов на доступ к персональным данным

6.1. В случае выявления неточных персональных данных при обращении субъекта персональных или его представителя либо по их запросу или по запросу уполномоченного

органа по защите прав субъектов персональных данных Оператор блокирует персональные данные, относящихся к этому субъекту персональных данных, или обеспечивает их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению Оператора) с момента такого обращения или получения указанного запроса на период проверки, если блокирование персональных данных не нарушает права и законные интересы субъекта персональных данных или третьих лиц.

6.2. В случае подтверждения факта неточности персональных данных Оператор на основании сведений, представленных субъектом персональных данных или его представителем либо уполномоченным органом по защите прав субъектов персональных данных, или иных необходимых документов обязан уточнить персональные данные либо обеспечить их уточнение (если обработка персональных данных осуществляется другим лицом, действующим по поручению Оператора) в течение семи рабочих дней со дня представления таких сведений и снять блокирование персональных данных.

6.3. В случае выявления неправомерной обработки персональных данных Оператор на период проверки блокирует неправомерно обрабатываемые персональные данные или обеспечивает их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению Оператора) с момента получения соответствующего запроса субъекта персональных данных или его представителя либо уполномоченного органа по защите прав субъектов персональных данных.

В случае выявления неправомерной обработки персональных данных, Оператор в срок, не превышающий трех рабочих дней с даты этого выявления, обязан прекратить неправомерную обработку персональных данных или обеспечить прекращение неправомерной обработки персональных данных лицом, действующим по поручению Оператора.

В случае, если обеспечить правомерность обработки персональных данных невозможно, Оператор в срок, не превышающий десяти рабочих дней с даты выявления неправомерной обработки персональных данных, обязан уничтожить такие персональные данные или обеспечить их уничтожение.

6.4. Об устранении допущенных нарушений или об уничтожении персональных данных Оператор уведомляет субъекта персональных данных или его представителя, а в случае, если обращение было направлено уполномоченным органом по защите прав субъектов персональных данных, также указанный орган.

6.5. В случае отзыва субъектом персональных данных согласия на обработку его персональных данных или достижения цели обработки персональных данных, а также по истечении срока, предусмотренного законом, договором, или согласием субъекта персональных данных на обработку его персональных данных, Оператор прекращает обработку персональных данных и производит их уничтожение, или обеспечивает прекращение обработки и уничтожение персональных данных, которые обрабатывались третьими лицами на основании договора с Оператором, в порядке и сроки, установленные законодательством Российской Федерации. При отзыве субъектом персональных данных согласия на обработку его персональных данных обработка осуществляется только в пределах, необходимых для исполнения заключенных с ним договоров и в целях, предусмотренных законодательством Российской Федерации.

7. **Обеспечение конфиденциальности персональных данных**

7.1. Обработка персональных данных осуществляется Оператором с соблюдением конфиденциальности, под которой понимается обязанность не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено законодательством Российской Федерации.

7.2. Оператор обеспечивает соблюдение конфиденциальность персональных данных со стороны своих работников, имеющих доступ к персональным данным, а также использование персональных данных работниками исключительно в целях, соответствующих закону, договору или иному соглашению, заключенному с субъектом персональных данных.

7.3. Защите подлежит информация содержащая персональные данные субъекта вне зависимости от способа ее обработки (как автоматизированной, так и обработки, осуществляемой без использования средств автоматизации либо смешанной обработке персональных данных).

7.4. Защита персональных данных, обрабатываемых в информационных системах персональных данных Оператора, от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий, обеспечивается Системой защиты персональных данных Оператора, в том числе включающей в себя программные и аппаратные средства защиты информации, с учетом требований законодательства, регламентирующего обработку персональных данных.

8. Меры, применяемые для защиты обрабатываемых персональных данных

8.1. Общество принимает необходимые и достаточные организационные и технические меры для защиты обрабатываемых персональных данных от неправомерного или случайного доступа, от уничтожения, изменения, блокирования, копирования, распространения, а также от иных неправомерных действий с ними со стороны третьих лиц. К таким мерам, в частности, относятся:

- назначение сотрудника, ответственного за организацию обработки персональных данных;
- осуществление внутреннего контроля соответствия обработки персональных данных Федеральному закону № 152-ФЗ;
- ознакомление работников, непосредственно осуществляющих обработку персональных данных, с положениями действующего законодательства о персональных данных, требованиями к защите персональных данных и иными документами по вопросам обработки персональных данных;
- определение угроз безопасности персональных данных при их обработке в информационных системах персональных данных;
- применение средств защиты информации, прошедших в установленном порядке процедуру оценки соответствия;
- осуществление учета носителей персональных данных;
- установление правил доступа к персональным данным, обрабатываемым в информационных системах персональных данных;
- осуществление контроля за принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности информационных систем персональных данных;
- разработка локальных актов по вопросам обработки персональных данных.

9. Заключительные положения

8.1. Настоящая Политика вступает в силу с момента утверждения и действует бессрочно.
8.2. Все работники Общества, участвующие в обработке персональных данных, несут ответственность за выполнение настоящей Политики в соответствии с действующим законодательством РФ, и знакомятся с данным документом под роспись.
8.3. Изменения в настоящую Политику могут быть внесены приказом генерального директора Общества, либо путем утверждения Политики в новой редакции.
8.4. Дополнительная информация по обработке и защите персональных данных может содержаться в других локальных нормативных документах, утвержденных в Обществе.
8.5. Актуальная версия Политики находится в свободном доступе на информационной стойке регистратуры Общества, а также расположена на официальном сайте Общества.
8.6. На сайте могут быть размещены ссылки на сторонние сайты и службы, которые не контролируются Оператором. Оператор не несет ответственности за безопасность или конфиденциальность любой информации, собираемой сторонними сайтами или службами.