

УТВЕРЖДЕНО
приказом Генерального директора
ООО «КлиНикаПроф»
от «01» января 2026 г. № 02-ПДн
В.В. Догадкин



ПОЛОЖЕНИЕ

**об обработке и защите персональных данных
в Обществе с ограниченной ответственностью «КлиНикаПроф»**

г. Клин, Московская область
2026 г.

1. Общие положения

1.1. Настоящее Положение об обработке и защите персональных данных (далее — Положение) определяет политику Общества с ограниченной ответственностью «КлиНикаПроф» (далее — Оператор, Общество) в отношении обработки персональных данных, устанавливает цели, правовые основания, объём, порядок и условия обработки персональных данных, а также реализуемые Оператором требования к защите персональных данных.

1.2. Положение разработано в соответствии с:

- Конституцией Российской Федерации;
- Трудовым кодексом Российской Федерации (глава 14);
- Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных»;
- Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федеральным законом от 21.11.2011 № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации» (в том числе статьями 13, 20, 92, 94);
- Федеральным законом от 29.11.2010 № 326-ФЗ «Об обязательном медицинском страховании в Российской Федерации»;
- 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 РФ от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;
- приказом ФСТЭК России от 18.02.2013 № 21 «Об утверждении Составы и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;
- приказом Роскомнадзора от 27.10.2022 № 178 «Об утверждении Требований к оценке вреда, который может быть причинён субъектам персональных данных...»;
- приказом Роскомнадзора от 28.10.2022 № 179 «Об утверждении Требований к подтверждению уничтожения персональных данных»;
- иными нормативными правовыми актами Российской Федерации в сфере персональных данных и охраны здоровья граждан.

1.3. Настоящее Положение является общедоступным документом, определяющим политику Оператора в отношении обработки персональных данных, в смысле части 2 статьи 18.1 Федерального закона № 152-ФЗ, и подлежит опубликованию в сети «Интернет» на официальном сайте Оператора по адресу клиникалин.рф с обеспечением неограниченного доступа к нему.

1.4. Действие Положения распространяется на все персональные данные, обрабатываемые Оператором как с использованием средств автоматизации, так и без

использования таких средств, включая обработку персональных данных на бумажных носителях (медицинская документация, кадровые документы, договоры).

1.5. Требования Положения обязательны для всех работников Оператора, а также для лиц, привлекаемых по гражданско-правовым договорам, которым в силу их обязанностей предоставлен доступ к персональным данным.

1.6. Сведения об Операторе:

- полное наименование: Общество с ограниченной ответственностью «КлиНикаПроф»;
- адрес: 141612, Московская область, г. Клин, ул. Карла Маркса, д. 101;
- ИНН / ОГРН: 5020072161 / 1135020000048;
- адрес электронной почты для обращений по вопросам обработки персональных данных: medicine_klin@mail.ru ;
- сведения об Операторе внесены в Реестр операторов, осуществляющих обработку персональных данных, регистрационный номер 77-18-011436.

2. Основные понятия

2.1. В настоящем Положении используются понятия в значениях, установленных статьёй 3 Федерального закона № 152-ФЗ, в частности:

- персональные данные — любая информация, относящаяся к прямо или косвенно определённом или определяемому физическому лицу (субъекту персональных данных);
- обработка персональных данных — любое действие (операция) или совокупность действий с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение;
- специальные категории персональных данных — данные, касающиеся состояния здоровья, интимной жизни, расовой и национальной принадлежности, политических взглядов, религиозных и философских убеждений, а также сведения о судимости;
- биометрические персональные данные — сведения, характеризующие физиологические и биологические особенности человека, на основании которых можно установить его личность и которые используются Оператором для установления личности субъекта;
- информационная система персональных данных (ИСПДн) — совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств;
- врачебная тайна — сведения о факте обращения гражданина за оказанием медицинской помощи, состоянии его здоровья и диагнозе, иные сведения, полученные при его медицинском обследовании и лечении (статья 13 Федерального закона № 323-ФЗ).

2.2. Все сведения о пациентах, обрабатываемые Оператором, одновременно составляют врачебную тайну и относятся к специальным категориям персональных данных, в связи с чем к ним применяется усиленный режим защиты, установленный настоящим Положением.

3. Категории субъектов и состав обрабатываемых персональных данных

3.1. Оператор обрабатывает персональные данные следующих категорий субъектов:

№	Категория субъектов	Состав обрабатываемых персональных данных
1	Пациенты (получатели медицинских услуг)	Фамилия, имя, отчество; пол; дата и место рождения; гражданство; адрес регистрации и фактического проживания; реквизиты документа, удостоверяющего личность; СНИЛС; полис ОМС/ДМС и наименование страховой организации; контактный телефон; адрес электронной почты; сведения о состоянии здоровья (жалобы, анамнез, диагнозы, результаты обследований и лечения, назначения, данные медицинских изображений); сведения об оказанных услугах и оплате
2	Законные представители пациентов, сопровождающие лица	Фамилия, имя, отчество; реквизиты документа, удостоверяющего личность; сведения о родстве или основании представительства; контактный телефон; адрес электронной почты
3	Работники Оператора	Сведения, предусмотренные Трудовым кодексом РФ и унифицированными формами кадрового учёта: ФИО, дата и место рождения, паспортные данные, адрес, СНИЛС, ИНН, сведения об образовании, квалификации, аккредитации и сертификатах специалиста, трудовой деятельности, воинском учёте, семейном положении (для налоговых вычетов и гарантий), сведения о доходах, данные личной медицинской книжки и результатов обязательных медицинских осмотров, банковские реквизиты для перечисления заработной платы
4	Кандидаты на замещение вакантных должностей	ФИО, дата рождения, контактные данные, сведения об образовании, квалификации и опыте работы, иные сведения, добровольно предоставленные кандидатом в резюме
5	Представители контрагентов, физические лица — стороны договоров	ФИО, должность, контактные данные, реквизиты документа, удостоверяющего личность, банковские реквизиты (для физических лиц и индивидуальных предпринимателей)
6	Посетители официального сайта клиникалин.рф	Данные, указанные субъектом в веб-формах записи и обратной связи (ФИО, номер телефона, адрес электронной почты, желаемая услуга/специалист, дата и время приёма, текст обращения); данные, автоматически передаваемые браузером и сервисами веб-аналитики: IP-адрес, файлы cookie, идентификатор пользователя (посетителя) метрической программы, сведения о браузере и операционной системе, дата и время доступа, источник перехода, просмотренные страницы

№	Категория субъектов	Состав обрабатываемых персональных данных
7	Лица, обратившиеся с отзывами, жалобами и обращениями	ФИО, контактные данные, содержание обращения и сведения, добровольно сообщённые заявителем
8	Лица, находящиеся в зоне видеонаблюдения	Изображение (видеозапись), дата и время фиксации

3.2. Оператор не обрабатывает биометрические персональные данные в целях установления личности субъекта. Фотографические изображения, содержащиеся в медицинской документации (в том числе фотографии зубных рядов, кожных покровов, результаты медицинской визуализации), обрабатываются исключительно в медицинских целях и не используются для идентификации личности, в связи с чем не относятся к биометрическим персональным данным.

3.3. Оператор не осуществляет обработку персональных данных, касающихся расовой и национальной принадлежности, политических взглядов, религиозных и философских убеждений, за исключением случаев, когда такие сведения сообщены пациентом и имеют клиническое значение (например, при определении показаний и противопоказаний, особенностей питания или гемотрансфузии).

3.4. Оператор не осуществляет обработку персональных данных несовершеннолетних иначе как с согласия их законных представителей, за исключением случаев оказания медицинской помощи в экстренной форме и иных случаев, прямо предусмотренных статьями 20 и 54 Федерального закона № 323-ФЗ.

4. Цели обработки персональных данных

4.1. Оператор обрабатывает персональные данные исключительно в заранее определённых и законных целях. Объём и содержание обрабатываемых данных соответствуют заявленным целям и не являются избыточными по отношению к ним.

4.2. Цели обработки персональных данных:

- оказание медицинской помощи и медицинских услуг, включая профилактику, диагностику, лечение, медицинскую реабилитацию, проведение медицинских осмотров и экспертиз;
- ведение и хранение медицинской документации в формах, установленных Министерством здравоохранения Российской Федерации;
- заключение, исполнение и прекращение договоров об оказании платных медицинских услуг, стороной, выгодоприобретателем или поручителем, по которым является субъект персональных данных;
- осуществление записи на приём, подтверждение, перенос и отмена приёма, информирование пациента о ходе и результатах оказания услуг;
- осуществление расчётов за оказанные услуги, оформление кассовых и бухгалтерских документов, выдача документов для получения социального налогового вычета;

- информационное взаимодействие со страховыми медицинскими организациями и страховщиками по договорам добровольного медицинского страхования, включая формирование счетов, реестров и предоставление медицинской документации для медико-экономической экспертизы и экспертизы качества медицинской помощи;
- осуществление внутреннего контроля качества и безопасности медицинской деятельности;
- ведение персонифицированного учёта сведений в сфере здравоохранения и представление сведений в государственные информационные системы в сфере здравоохранения (ЕГИСЗ, ЕМИАС, РЭМД, ФРМР, ФРМО) в объёме и порядке, установленных законодательством;
- исполнение обязанностей по представлению отчётности и сведений в органы государственной власти, органы контроля и надзора, фонды, налоговые органы, органы дознания и следствия, суды — в случаях и объёме, предусмотренных законодательством;
- организация кадрового учёта и делопроизводства, обеспечение соблюдения законодательства о труде, начисление и выплата заработной платы, предоставление гарантий и компенсаций, обеспечение обязательного социального и медицинского страхования работников;
- обеспечение допуска работников к осуществлению медицинской деятельности, проверка наличия действующей аккредитации специалиста, проведение обязательных предварительных и периодических медицинских осмотров;
- подбор персонала и рассмотрение кандидатур на замещение вакантных должностей;
- заключение и исполнение договоров с контрагентами, ведение претензионной и договорной работы;
- рассмотрение обращений, отзывов, заявлений и жалоб субъектов персональных данных и подготовка ответов на них;
- защита прав и законных интересов Оператора, в том числе в досудебном и судебном порядке;
- обеспечение функционирования официального сайта клиникаclin.рф, обработка заявок, направляемых через формы обратной связи и формы онлайн-записи;
- сбор и анализ обезличенной статистики посещений сайта с использованием метрических программ (сервисов веб-аналитики) в целях улучшения работы сайта и качества обслуживания;
- направление субъекту информационных и рекламных сообщений о медицинских услугах Оператора — исключительно при наличии отдельного предварительного согласия субъекта, оформленного в соответствии со статьёй 18 Федерального закона «О рекламе»;
- обеспечение имущественной безопасности, безопасности пациентов и работников путём видеонаблюдения в помещениях общего пользования и на прилегающей территории.

4.3. Обработка персональных данных в целях, не указанных в пункте 4.2 настоящего Положения, не допускается. При возникновении новой цели обработки Оператор до начала обработки вносит соответствующие изменения в настоящее Положение и направляет в Роскомнадзор уведомление об изменении сведений, содержащихся в Реестре операторов.

5. Правовые основания обработки

5.1. Правовыми основаниями обработки персональных данных являются:

- Федеральный закон от 21.11.2011 № 323-ФЗ, приказы Министерства здравоохранения Российской Федерации, устанавливающие порядки оказания медицинской помощи, формы и правила ведения медицинской документации (в том числе приказы Минздрава России от 15.12.2014 № 834н, от 05.08.2022 № 530н), правила предоставления платных медицинских услуг;
- Трудовой кодекс Российской Федерации, Налоговый кодекс Российской Федерации, федеральные законы об обязательном пенсионном, социальном и медицинском страховании, законодательство об архивном деле;
- Устав Общества, лицензия на осуществление медицинской деятельности, договоры об оказании платных медицинских услуг, договоры с контрагентами и страховыми организациями;
- согласия субъектов персональных данных на обработку персональных данных, оформленные в соответствии со статьями 9 и 10 Федерального закона № 152-ФЗ;
- информированные добровольные согласия на медицинское вмешательство, оформляемые в соответствии со статьёй 20 Федерального закона № 323-ФЗ;
- согласия на обработку персональных данных, разрешённых субъектом для распространения (статья 10.1 Федерального закона № 152-ФЗ), — при размещении сведений о работниках на сайте Оператора;
- настоящее Положение и иные локальные нормативные акты Оператора.

5.2. Обработка специальных категорий персональных данных, касающихся состояния здоровья, осуществляется Оператором в медико-профилактических целях, в целях установления медицинского диагноза, оказания медицинских услуг при условии, что обработка осуществляется лицом, профессионально занимающимся медицинской деятельностью и обязанным сохранять врачебную тайну (пункт 4 части 2 статьи 10 Федерального закона № 152-ФЗ), а также на основании согласия субъекта персональных данных.

5.3. Согласие субъекта персональных данных оформляется отдельно от иных документов и не может быть включено в текст договора, информированного добровольного согласия на медицинское вмешательство, анкеты или иного документа. Согласие должно быть конкретным, предметным, информированным, сознательным и однозначным. Не допускается включение в согласие положений, влекущих неоднозначное толкование, а также объединение в одном согласии разных, несовместимых между собой целей обработки.

5.4. Оператор не вправе отказать пациенту в оказании медицинских услуг в случае отказа субъекта дать согласие на обработку персональных данных в целях, не связанных с оказанием медицинской помощи (в частности, в рекламных и маркетинговых целях).

5.5. Обязанность предоставить доказательство получения согласия субъекта персональных данных, а при обработке специальных категорий — доказательство наличия предусмотренных законом оснований, возлагается на Оператора.

6. Принципы и условия обработки

6.1. Обработка персональных данных осуществляется на законной и справедливой основе, ограничивается достижением конкретных, заранее определённых и законных целей.

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

6.3. Обрабатываются только те персональные данные, которые отвечают целям их обработки. Содержание и объём обрабатываемых данных соответствуют заявленным целям; избыточность не допускается.

6.4. Оператор обеспечивает точность персональных данных, их достаточность, а в необходимых случаях — актуальность. Оператор принимает необходимые меры по удалению или уточнению неполных или неточных данных.

6.5. Хранение персональных данных осуществляется в форме, позволяющей определить субъекта, не дольше, чем этого требуют цели обработки, если срок хранения не установлен федеральным законом или договором. Обрабатываемые данные подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей.

6.6. Сбор, запись, систематизация, накопление, хранение, уточнение и извлечение персональных данных граждан Российской Федерации осуществляются с использованием баз данных, находящихся на территории Российской Федерации (часть 5 статьи 18 Федерального закона № 152-ФЗ). Оператор обеспечивает размещение медицинской информационной системы, системы онлайн-записи и сайта на серверах, расположенных на территории Российской Федерации.

6.7. Оператор не принимает решений, порождающих юридические последствия в отношении субъекта персональных данных или иным образом затрагивающих его права и законные интересы, на основании исключительно автоматизированной обработки персональных данных.

7. Особенности обработки персональных данных на официальном сайте

7.1. На официальном сайте Оператора клиникаclin.rf обрабатываются персональные данные, предоставленные посетителями сайта через формы онлайн-записи и обратной связи, а также данные, автоматически собираемые при использовании сайта.

7.2. Отправка любой формы на сайте возможна только после самостоятельного проставления посетителем отметки (чек-бокса) о согласии на обработку персональных

данных. Отметка не может быть проставлена заранее (по умолчанию). Рядом с отметкой размещается активная ссылка на текст согласия и на настоящее Положение.

7.3. На сайте применяются метрические программы (сервисы веб-аналитики), обрабатывающие файлы cookie и иные идентификаторы посетителей. При первом посещении сайта посетителю отображается информационное уведомление об использовании файлов cookie с возможностью ознакомиться с политикой их использования. Данные веб-аналитики обрабатываются в целях сбора статистики посещений и улучшения работы сайта; в Реестре операторов данная обработка отражена с указанием категории субъектов «посетители сайта» и способа обработки с использованием метрических программ.

7.4. Оператор не использует сервисы веб-аналитики и иные сервисы, предполагающие передачу персональных данных на серверы, расположенные за пределами Российской Федерации, без предварительного направления в Роскомнадзор уведомления о трансграничной передаче персональных данных и получения соответствующего подтверждения в случаях, предусмотренных статьёй 12 Федерального закона № 152-ФЗ.

7.5. На сайте в постоянном доступе (в том числе в подвале всех страниц) размещаются: настоящее Положение, форма (текст) согласия на обработку персональных данных, политика в отношении файлов cookie, пользовательское соглашение, сведения об Операторе и его лицензии, а также иные сведения, обязательные к раскрытию в соответствии с Правилами предоставления медицинскими организациями платных медицинских услуг.

7.6. Персональные данные, поступающие через формы сайта, передаются по защищённому протоколу (HTTPS) и поступают в информационные системы Оператора, размещённые на территории Российской Федерации. Направление таких данных на внешние адреса электронной почты, размещённые на иностранных почтовых сервисах, не допускается.

8. Передача персональных данных третьим лицам

8.1. Оператор не раскрывает третьим лицам и не распространяет персональные данные без согласия субъекта, если иное не предусмотрено федеральным законом.

8.2. Предоставление сведений, составляющих врачебную тайну, без согласия гражданина или его законного представителя допускается исключительно в случаях, прямо перечисленных в части 4 статьи 13 Федерального закона № 323-ФЗ.

8.3. Оператор вправе поручить обработку персональных данных другому лицу с согласия субъекта персональных данных на основании заключаемого договора (поручения оператора). Поручение в обязательном порядке содержит перечень действий с персональными данными, цели обработки, обязанность соблюдать конфиденциальность, требования к защите обрабатываемых данных, обязанность по запросу Оператора в течение срока действия поручения направлять сведения о выполнении требований статьи 19 Федерального закона № 152-ФЗ, а также обязанность уведомлять Оператора об инцидентах в течение 24 часов.

8.4. Типовыми категориями лиц, которым может поручаться обработка либо которым передаются персональные данные, являются: страховые медицинские организации и страховщики по договорам ДМС; лаборатории и медицинские организации, привлекаемые для проведения отдельных исследований и консультаций; операторы медицинских информационных систем и IP-телефонии; операторы связи, осуществляющие рассылку сервисных сообщений; организации, обеспечивающие бухгалтерское и кадровое сопровождение; аудиторы и юридические консультанты; органы государственной власти в случаях, установленных законом.

8.5. Оператор несёт ответственность перед субъектом персональных данных за действия лица, которому поручена обработка. Лицо, осуществляющее обработку по поручению, несёт ответственность перед Оператором.

8.6. Трансграничная передача персональных данных осуществляется только после направления в Роскомнадзор соответствующего уведомления и с соблюдением требований статьи 12 Федерального закона № 152-ФЗ. По состоянию на дату утверждения настоящего Положения Оператор трансграничную передачу персональных данных не осуществляет.

9. Сроки обработки и хранения. Порядок уничтожения

9.1. Сроки обработки персональных данных определяются достижением целей обработки либо сроками, установленными законодательством Российской Федерации:

Категория документов (данных)	Срок хранения
Медицинская карта пациента, получающего медицинскую помощь в амбулаторных условиях, и иная первичная медицинская документация	В соответствии с приказом Минздрава России от 05.08.2022 № 530н — 25 лет (для отдельных видов документации — иные сроки, установленные указанным приказом)
Информированные добровольные согласия на медицинское вмешательство	Хранятся в составе медицинской документации в соответствующий срок
Договоры об оказании платных медицинских услуг и первичные учётные документы	5 лет после окончания отчётного года, если иной срок не установлен законодательством о бухгалтерском учёте и налогах
Кадровые документы, личные дела работников	50 лет (для документов, законченных делопроизводством после 01.01.2003), 75 лет — для более ранних
Данные кандидатов, не принятых на работу	Не более 3 лет с момента получения, если субъектом не дано иное согласие
Согласия на обработку персональных данных	3 года с даты истечения срока действия согласия или его отзыва
Заявки и обращения, поступившие через сайт	Не более 1 года с момента получения, если данные не включены в медицинскую документацию
Данные веб-аналитики и файлы cookie	В соответствии со сроками, установленными правообладателем сервиса веб-аналитики, но не более 1 года

Категория документов (данных)	Срок хранения
Записи системы видеонаблюдения	30 календарных дней, если запись не изъята в установленном порядке или не требуется для рассмотрения обращения либо спора

9.2. В случае достижения цели обработки, отзыва субъектом согласия при отсутствии иных правовых оснований, а также выявления неправомерной обработки Оператор прекращает обработку и уничтожает персональные данные в срок, не превышающий тридцати дней с даты наступления соответствующего обстоятельства, если иной срок не установлен федеральным законом.

9.3. Уничтожение персональных данных оформляется актом об уничтожении персональных данных, составляемым комиссией, назначаемой приказом генерального директора. При уничтожении данных, содержащихся в информационной системе, дополнительно оформляется выгрузка из журнала регистрации событий в информационной системе. Требования к подтверждению уничтожения установлены приказом Роскомнадзора от 28.10.2022 № 179; акты и выгрузки хранятся не менее трёх лет.

9.4. Отзыв субъектом согласия на обработку персональных данных не влечёт прекращения обработки тех данных, обработка которых осуществляется на иных правовых основаниях, в том числе в целях исполнения обязанности по ведению и хранению медицинской документации в установленные законом сроки. Об этом субъекту сообщается в ответе на его обращение с указанием конкретного правового основания продолжения обработки.

10. Права субъектов персональных данных

10.1. Субъект персональных данных имеет право:

- получать информацию, касающуюся обработки его персональных данных, в объёме, предусмотренном частью 7 статьи 14 Федерального закона № 152-ФЗ;
- требовать уточнения своих персональных данных, их блокирования или уничтожения в случае, если они являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки;
- отозвать согласие на обработку персональных данных;
- возражать против обработки персональных данных в целях продвижения услуг на рынке;
- обжаловать действия или бездействие Оператора в Роскомнадзор или в судебном порядке;
- на защиту своих прав и законных интересов, в том числе на возмещение убытков и компенсацию морального вреда.

10.2. Обращения субъектов направляются в письменной форме по адресу Оператора либо по адресу электронной почты, указанному в пункте 1.6 настоящего Положения. Запрос должен содержать сведения, предусмотренные частью 3 статьи 14 Федерального закона № 152-ФЗ: номер основного документа, удостоверяющего личность субъекта или его

представителя, сведения о дате выдачи и выдавшем органе, сведения, подтверждающие участие субъекта в отношениях с Оператором, подпись субъекта или его представителя. Запрос может быть направлен в форме электронного документа, подписанного электронной подписью.

10.3. Сроки рассмотрения обращений:

- предоставление сведений об обработке персональных данных или мотивированного отказа — в течение десяти рабочих дней с даты получения запроса; срок может быть продлён, но не более чем на пять рабочих дней, с направлением субъекту уведомления с обоснованием продления;
- внесение необходимых изменений в персональные данные при представлении субъектом подтверждающих сведений — в течение семи рабочих дней, с уведомлением субъекта и третьих лиц, которым данные передавались;
- прекращение неправомерной обработки — в срок, не превышающий трёх рабочих дней с даты выявления;
- уничтожение персональных данных — в срок, не превышающий тридцати дней.

10.4. Оператор вправе ограничить доступ субъекта к его персональным данным в случаях, предусмотренных частью 8 статьи 14 Федерального закона № 152-ФЗ. Отказ должен быть мотивированным и оформляться в письменной форме.

10.5. Ознакомление пациента с медицинской документацией и получение её копий осуществляется в порядке, установленном статьёй 22 Федерального закона № 323-ФЗ и приказом Министерства здравоохранения Российской Федерации, устанавливающим соответствующий порядок.

11. Меры по обеспечению безопасности персональных данных

11.1. Во исполнение части 1 статьи 18.1 и статьи 19 Федерального закона № 152-ФЗ Оператор принимает следующие организационные меры:

- назначает лицо, ответственное за организацию обработки персональных данных;
- издаёт настоящее Положение и иные локальные нормативные акты по вопросам обработки и защиты персональных данных, перечень которых приведён в разделе 14;
- утверждает перечень должностей работников, замещение которых предусматривает осуществление обработки персональных данных либо доступ к ним;
- утверждает перечень информационных систем персональных данных и мест хранения материальных носителей;
- осуществляет внутренний контроль соответствия обработки персональных данных требованиям законодательства не реже одного раза в год;
- проводит оценку вреда, который может быть причинён субъектам персональных данных, в соответствии с приказом Роскомнадзора от 27.10.2022 № 178, и соотносит его с принимаемыми мерами защиты;

- определяет угрозы безопасности персональных данных и уровень защищённости при их обработке в информационных системах;
- обеспечивает ознакомление работников, непосредственно осуществляющих обработку персональных данных, с положениями законодательства, настоящим Положением и иными локальными актами, а также проводит обучение работников;
- получает от работников обязательства о неразглашении сведений, составляющих врачебную тайну и содержащих персональные данные;
- обеспечивает опубликование настоящего Положения на сайте Оператора и возможность ознакомления с ним неограниченного круга лиц.

11.2. Технические меры защиты включают:

- определение уровня защищённости персональных данных при их обработке в информационных системах и применение мер, предусмотренных постановлением Правительства РФ № 1119 и приказом ФСТЭК России № 21. С учётом обработки специальных категорий персональных данных субъектов, не являющихся работниками Оператора, устанавливается уровень защищённости, определяемый актом классификации ИСПДн;
- идентификацию и аутентификацию пользователей, разграничение прав доступа по принципу минимально необходимых полномочий, персонифицированные учётные записи (использование общих учётных записей не допускается);
- регистрацию и учёт действий пользователей в информационных системах, ведение журналов событий безопасности;
- применение сертифицированных средств антивирусной защиты и средств межсетевого экранирования;
- использование зашифрованных каналов связи (HTTPS, VPN) при передаче персональных данных по сетям общего пользования;
- резервное копирование данных с обеспечением защиты резервных копий и их хранением на территории Российской Федерации;
- контроль съёмных машинных носителей информации, их учёт и обезличенную маркировку;
- обнаружение фактов несанкционированного доступа к персональным данным и принятие мер по восстановлению модифицированных или уничтоженных данных.

11.3. Организационные меры при обработке персональных данных без использования средств автоматизации (постановление Правительства РФ № 687):

- раздельное хранение материальных носителей, обработка которых осуществляется в разных целях;
- хранение медицинской и кадровой документации в запираемых шкафах (сейфах) в помещениях, доступ в которые ограничен;
- запрет оставлять документы, содержащие персональные данные, в местах, доступных для посторонних лиц, включая рабочие столы в зонах приёма пациентов и стойку регистратуры;

- обеспечение конфиденциальности при вызове пациента и при взаимодействии с ним в регистратуре: не допускается оглашение диагноза и иных сведений, составляющих врачебную тайну, в присутствии третьих лиц;
- уничтожение документов, содержащих персональные данные, способом, исключающим восстановление информации (шредирование).

11.4. Доступ работников к персональным данным предоставляется в объёме, необходимом для исполнения их трудовой функции, на основании утверждённого перечня должностей. Передача пароля другому лицу, вход в информационную систему под чужой учётной записью, копирование персональных данных на личные устройства и в личные учётные записи, а также передача персональных данных с использованием личных мессенджеров и почтовых сервисов не допускаются.

12. Ответственный за организацию обработки персональных данных

12.1. Ответственный за организацию обработки персональных данных назначается приказом генерального директора и подчиняется непосредственно генеральному директору.

12.2. Ответственный:

- осуществляет внутренний контроль соблюдения Оператором и его работниками законодательства о персональных данных, в том числе требований к их защите;
- доводит до сведения работников положения законодательства о персональных данных, локальных актов Оператора, требований к защите персональных данных;
- организует приём и обработку обращений и запросов субъектов персональных данных и их представителей, осуществляет контроль за приёмом и обработкой таких обращений;
- организует подготовку и направление в Роскомнадзор уведомления об обработке персональных данных и уведомлений об изменении сведений, содержащихся в реестре;
- организует проведение оценки вреда субъектам персональных данных и её актуализацию;
- участвует в расследовании инцидентов и организует направление уведомлений в уполномоченный орган.

12.3. Оператор обязан направлять в Роскомнадзор уведомление об изменении сведений, содержащихся в реестре, не позднее пятнадцатого числа месяца, следующего за месяцем, в котором произошли изменения (в том числе при изменении целей обработки, категорий субъектов, состава обрабатываемых данных, сведений об ответственном лице, адреса Оператора, а также при начале использования новых сервисов, обрабатывающих персональные данные).

13. Порядок реагирования на инциденты

13.1. Инцидентом признаётся неправомерная или случайная передача (предоставление, распространение, доступ) персональных данных, повлёкшая нарушение

прав субъектов персональных данных, а также неправомерный доступ к персональным данным.

13.2. Работник, обнаруживший признаки инцидента, обязан незамедлительно сообщить о нём ответственному за организацию обработки персональных данных и непосредственному руководителю.

13.3. Оператор в течение двадцати четырёх часов с момента выявления инцидента направляет в Роскомнадзор уведомление с указанием предполагаемой причины инцидента, предполагаемого вреда правам субъектов, принятых мер по устранению последствий и сведений о лице, уполномоченном на взаимодействие с уполномоченным органом.

13.4. В течение семидесяти двух часов с момента выявления инцидента Оператор направляет уведомление о результатах внутреннего расследования, включая сведения о лицах, действия которых стали причиной инцидента (при наличии).

13.5. Оператор во взаимодействии с ГосСОПКА обеспечивает передачу сведений об инциденте в порядке, установленном законодательством.

13.6. По итогам расследования ответственный за организацию обработки персональных данных готовит заключение с перечнем корректирующих мер, которые утверждаются генеральным директором.

14. Перечень локальных актов и форм документов

14.1. Настоящее Положение применяется совместно со следующими документами Оператора:

№	Документ	Форма утверждения
1	Приказ о назначении лица, ответственного за организацию обработки персональных данных, и лица, ответственного за обеспечение безопасности персональных данных в ИСПДн	Приказ
2	Приказ об утверждении настоящего Положения и введении его в действие	Приказ
3	Перечень персональных данных, обрабатываемых Оператором в связи с реализацией трудовых отношений и в связи с оказанием медицинских услуг	Приложение к приказу
4	Перечень должностей, замещение которых предусматривает осуществление обработки персональных данных либо доступ к ним	Приложение к приказу
5	Перечень информационных систем персональных данных и мест хранения материальных носителей	Приложение к приказу
6	Акт определения уровня защищённости персональных данных при их обработке в ИСПДн	Акт, утверждаемый приказом
7	Модель угроз безопасности персональных данных	Утверждается приказом
8	Акт оценки вреда, который может быть причинён субъектам персональных данных	Акт, утверждаемый приказом

№	Документ	Форма утверждения
9	Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям законодательства	Приложение к приказу
10	Правила работы с материальными носителями персональных данных и порядок их уничтожения; форма акта об уничтожении персональных данных	Приложение к приказу
11	Правила рассмотрения запросов субъектов персональных данных и их представителей; журнал учёта обращений	Приложение к приказу
12	Инструкция пользователя ИСПДн и инструкция администратора безопасности; парольная политика	Приложение к приказу
13	Порядок реагирования на инциденты (компьютерные инциденты) и взаимодействия с Роскомнадзором и ГосСОПКА	Приложение к приказу
14	Обязательство работника о неразглашении персональных данных и сведений, составляющих врачебную тайну	Форма, приложение к приказу
15	Форма согласия пациента на обработку персональных данных (отдельный документ)	Форма, приложение к приказу
16	Форма согласия работника на обработку персональных данных и согласия на обработку персональных данных, разрешённых для распространения	Форма, приложение к приказу
17	Форма согласия на получение информационных и рекламных сообщений	Форма, приложение к приказу
18	Согласие на обработку персональных данных, размещаемое на сайте, и Политика в отношении файлов cookie	Публикуются на сайте
19	Журнал учёта машинных носителей персональных данных; журнал учёта передачи персональных данных третьим лицам	Форма, приложение к приказу
20	Положение о видеонаблюдении и форма информационной таблички о ведении видеонаблюдения	Приложение к приказу

15. Ответственность

15.1. Работники Оператора, виновные в нарушении требований настоящего Положения и законодательства о персональных данных, несут дисциплинарную, материальную, административную, гражданско-правовую и уголовную ответственность в соответствии с законодательством Российской Федерации.

15.2. Разглашение персональных данных, ставших известными работнику в связи с исполнением им трудовых обязанностей, в том числе сведений, составляющих врачебную тайну, является основанием для расторжения трудового договора по инициативе работодателя в соответствии с подпунктом «в» пункта 6 части 1 статьи 81 Трудового кодекса Российской Федерации.

15.3. Административная ответственность за нарушения в области обработки персональных данных установлена статьёй 13.11 Кодекса Российской Федерации об административных правонарушениях, уголовная — статьями 137 и 272.1 Уголовного кодекса Российской Федерации.

16. Заключительные положения

16.1. Настоящее Положение вступает в силу с момента его утверждения приказом генерального директора и действует бессрочно до замены новым Положением.

16.2. Положение подлежит пересмотру не реже одного раза в год, а также при изменении законодательства Российской Федерации, изменении целей, состава обрабатываемых персональных данных, применяемых информационных систем или организационной структуры Оператора.

16.3. Актуальная редакция Положения размещается на официальном сайте Оператора. Датой изменения Положения считается дата утверждения новой редакции приказом генерального директора.

16.4. Все работники Оператора, осуществляющие обработку персональных данных, подлежат ознакомлению с настоящим Положением под подпись. Лист ознакомления является неотъемлемой частью Положения.

Ответственный за организацию обработки персональных данных

_____/ Догадкин Владислав Владимирович /

«01» января 2026 г.

