

Общество с ограниченной ответственностью
«ТС Клиника» (ООО «ТС Клиника»)

Политика обработки персональных данных работников

ИТВЕРЖДАЮ
Директор
Караченко А.В.
"01" _____ 2023 г.



г. Краснодар

1. Общие положения

1.1. Настоящая политика в отношении обработки персональных данных (далее – Политика) разработана Обществом с ограниченной ответственностью «ТС Клиника» (далее – Оператор) в целях исполнения требований Федерального закона от 27.06.2006 № 152-ФЗ «О персональных данных».

1.2. Политика определяет общий порядок, принципы и условия обработки персональных данных Оператором и обеспечивает защиту прав субъектов персональных данных при обработке их персональных данных.

1.3. Целью настоящей Политики является обеспечение безопасности при обработке персональных данных. Безопасность персональных данных достигается путем исключения несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иные несанкционированные Оператором действия.

1.4. Настоящий документ является общедоступным, определяющим политику Оператора в отношении обработки персональных данных и содержащих сведения о реализуемых мерах по защите персональных данных.

1.5. Настоящая Политика является обязательным для исполнения документом всеми сотрудниками Оператора, имеющими доступ к обрабатываемым в ООО «ТС Клиника» персональным данным.

1.6. В Политике устанавливаются:

- цели, порядок и условия обработки персональных данных;
- категории субъектов, персональные данные которых обрабатываются, категории (перечни) обрабатываемых персональных данных при достижении целей обработки или при иных законных оснований;
- положения, касающиеся защиты персональных данных, процедуры, направленные на выявление и предотвращение нарушений законодательства РФ в области персональных данных, а также на устранение последствий таких нарушений

2. Основные понятия, используемые в Политике.

2.1. Основные понятия:

- персональные данные- любая информация, относящаяся к определенному или определяемому на основании такой информации работнику, в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация, необходимая работодателю в связи с трудовыми отношениями;
- оператор персональных данных (оператор). Учреждение, самостоятельно или совместно с другими лицами организующее и (или) осуществляющее обработку персональных данных, а также определяющее цели обработки, 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 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;
- конфиденциальность персональных данных. Обязательное для оператора и иных лиц, получивших доступ к персональным данным, требование не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.;
- распространение персональных данных- действия, направленные на передачу персональных данных работников определенному кругу лиц (передача персональных данных) или на ознакомление с персональными данными неограниченного круга лиц, в том числе обнародование персональных данных работников в средствах массовой информации, размещение в информационно- телекоммуникационных сетях или предоставление доступа к персональным данным работников каким-либо иным способом;
- информационная система персональных данных. Совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств;
- субъект персональных данных. Физическое лицо, данные которого обрабатываются;
- доступ к информации- возможность получения информации и с целью ее последующего использования (обработки);
- несанкционированный доступ (несанкционированные действия)- доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых информационными системами персональных данных;
- правила разграничения доступа- совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа;
- субъект доступа- лицо или процесс, действия которого регламентируются правилами разграничения доступа
- использование персональных данных- действия (операции) с персональными данными, совершаемые должностным лицом Работодателя в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении работников либо иным образом затрагивающих их права и свободы других лиц;
- блокирование персональных данных- временное прекращение сбора, систематизации, накопления, использования, распространения персональных данных работников, в том числе их передачи;
- уничтожение персональных данных- действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных работников;
- обезличивание персональных данных- действия, в результате которых невозможно определить принадлежность данных конкретному работнику;
- общедоступные персональные данные- персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия работника или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности;
- информация- сведения (сообщения, данные) независимо от формы их представления;
- документированная информация- зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию или ее материальный носитель.

3. Категории субъектов персональных данных

3.1. К субъектам, персональные данные которых обрабатываются Оператором в соответствии с Политикой, относятся:

- кандидаты для приема на работу к Оператору;
- работники Оператора;
- бывшие работники Оператора;
- члены семей работников Оператора- в случаях, когда согласно законодательству сведения о них предоставляются работником;
- Пациенты, законные представители пациентов.

4. Цели обработки персональных данных, категории (перечни) обрабатываемых персональных данных

4.1. Согласно Политике персональные данные обрабатываются с целью применения и исполнения трудового законодательства в рамках трудовых и иных непосредственно связанных с ними отношений, в том числе:

4.1.1. При содействии в трудоустройстве.

4.1.1.1. Категории и перечни персональных данных:

- фамилия, имя, отчество (при наличии), а также прежние фамилия, имя, отчество (при наличии);
 - пол;
 - дата (число, месяц, год) и место рождения;
 - сведения о гражданстве;
 - вид, серия, номер документа, удостоверяющего личность, наименование органа, выдавшего его, дата выдачи;
 - страховой номер индивидуального лицевого счета (СНИЛС);
 - идентификационный номер налогоплательщика (ИНН);
 - адрес и дата регистрации по месту жительства (место пребывания), адрес фактического проживания;
 - номер контактного телефона, адрес электронной почты и (или) сведения о других способах связи;
 - реквизиты свидетельств о государственной регистрации актов гражданского состояния и содержащиеся в них сведения;
 - сведения о семейном положении, составе семьи (степень родства, фамилии, имена, отчества (при наличии), даты (число, месяц, год) и места рождения);
 - сведения об образовании и (или) квалификации или наличии специальных знаний (в том числе наименование образовательной и (или) иной организации, год окончания, уровень образования, квалификация, реквизиты документа об образовании, обучении);
 - сведения об отношении к воинской обязанности, о воинском учете и реквизиты документов воинского учета (серия, номер, дата выдачи документа, наименование органа, выдавшего его);
 - сведения о трудовой деятельности, а также информация о предыдущих местах работы, периодах и стаже работы;
 - сведения, содержащиеся в документах, дающих право на пребывание и трудовую деятельность на территории РФ (для иностранных граждан, пребывающих в РФ);
- 4.1.1.2. Категории субъектов персональных данных:
- кандидаты для приема на работу к Оператору;
 - члены семей работников Оператора- в случаях, когда согласно законодательству сведения о них предоставляются работником.
- 4.1.1.3. Способы обработки персональных данных:
- автоматизированный и неавтоматизированный;
- 4.1.1.4. Сроки обработки и хранения данных:

- 30 календарных дней.

4.1.1.5. Порядок уничтожения.

4.1.1.5.1. Уничтожение персональных данных осуществляет комиссия, созданная приказом директора.

4.1.1.5.2. Комиссия составляет список с указанием документов, иных материальных носителей и (или) сведений в информационных системах, содержащих персональные данные, которые подлежат уничтожению.

4.1.1.5.3 Персональные данные на бумажных носителях уничтожаются с использованием shreddera. Персональные данные на электронных носителях уничтожаются путем механического нарушения целостности носителя, не позволяющего считать или восстановить персональные данные, а также путем удаления данных с электронных носителей методами и средствами гарантированного удаления остаточной информации.

4.1.1.5.4. Комиссия подтверждает уничтожение персональных данных, указанных в п.п. 4.1.1.1. Политики, согласно Требованиям к подтверждению уничтожения персональных данных, утвержденных Приказом Роскомнадзора от 28.10.2022 № 179, а именно:

- актом об уничтожении персональных данных- если данные обрабатываются без использования средств автоматизации;

- актом об уничтожении персональных данных и выгрузкой из журнала регистрации событий в информационной системе персональных данных- если данных обрабатываются с использованием средств автоматизации либо одновременно с использованием и без использования таких средств.

Акт может составляться на бумажном носителе или в электронной форме, подписанной электронными подписями.

Формы акта и выгрузки из журнала с учетом сведений, который должны содержаться в указанных документах, утверждаются приказом директора.

4.1.1.5.5. После составления акта об уничтожении персональных данных и выгрузки из журнала регистрации событий в информационной системе персональных данных комиссия передает их в общий отдел для последующего хранения. Акты и выгрузки из журнала хранятся в течение трех лет с момента уничтожения персональных данных.

4.1.2. Оформление трудовых отношений:

4.1.2.1. Категории и перечни персональных данных:

Информация, предоставляемая работником при поступлении на работу к Оператору, должна иметь документальную форму. При заключении трудового договора в соответствии со ст. 65 Трудового кодекса РФ лицо, поступающее на работу, предъявляет:

- паспорт или иной документ, удостоверяющий личность;

- трудовую книжку, за исключением случаев, когда договор заключается впервые, или работник поступает на работу на условиях совместительства, или трудовая книжка у работника отсутствует в связи с ее утратой или по другим причинам;

- результаты обязательных предварительных (при поступлении на работу) и периодических медицинских осмотров (обследований), а также обязательного психиатрического освидетельствования;

- страховое свидетельство государственного пенсионного страхования;

- документы воинского учета- для лиц, подлежащих воинскому учету;

- документ об образовании, о квалификации или наличии специальных знаний- при поступлении на работу, требующую специальных знаний или специальной подготовки;

- свидетельство о присвоении ИНН (при его наличии у работника).

При оформлении работника отделом кадров заполняется унифицированная форма Т-2 «Личная карточка работника», в которой отражаются следующие анкетные и биографические данные работника:

- общие сведения (Ф.И.О., дата рождения, гражданство, образование, профессия, стаж работы, состояние в браке, паспортные данные);

- сведения о воинском учете;

- данные о приеме на работу;
- сведения об аттестации;
- сведения о повышении квалификации;
- сведения о профессиональной переподготовке;
- сведения о наградах (поощрениях), почетных званиях;
- сведения об отпусках;
- сведения о социальных гарантиях;
- сведения о месте жительства и контактных телефонах.
- сведения о наличии (отсутствии) судимости и (или) факта уголовного преследования либо о прекращении уголовного преследования по реабилитирующим основаниям (для отдельных категорий работников)

4.1.2.2. Категории субъектов персональных данных

- кандидаты для приема на работу к Оператору;
- члены семей работников Оператора- в случаях, когда согласно законодательству сведения о них предоставляются работником.

4.1.2.3. Способы обработки персональных данных:

- автоматизированный и неавтоматизированный;

4.1.2.4. Сроки обработки и хранения данных:

- 50 лет .

4.1.2.5. Порядок уничтожения.

4.1.2.5.1. Уничтожение персональных данных осуществляет комиссия, созданная приказом директора.

4.1.2.5.2. Комиссия составляет список с указанием документов, иных материальных носителей и (или) сведений в информационных системах, содержащих персональные данные, которые подлежат уничтожению.

4.1.2.5.3 Персональные данные на бумажных носителях уничтожаются с использованием shreddera. Персональные данные на электронных носителях уничтожаются путем механического нарушения целостности носителя, не позволяющего считать или восстановить персональные данные, а также путем удаления данных с электронных носителей методами и средствами гарантированного удаления остаточной информации.

4.1.2.5.4. Комиссия подтверждает уничтожение персональных данных, указанных в п.п. 4.1.2.1. Политики, согласно Требованиям к подтверждению уничтожения персональных данных, утвержденных Приказом Роскомнадзора от 28.10.2022 № 179, а именно:

- актом об уничтожении персональных данных- если данные обрабатываются без использования средств автоматизации;

- актом об уничтожении персональных данных и выгрузкой из журнала регистрации событий в информационной системе персональных данных- если данных обрабатываются с использованием средств автоматизации либо одновременно с использованием и без использования таких средств.

Акт может составляться на бумажном носителе или в электронной форме, подписанной электронными подписями.

Формы акта и выгрузки из журнала с учетом сведений, который должны содержаться в указанных документах, утверждаются приказом директора.

4.1.2.5.5. После составления акта об уничтожении персональных данных и выгрузки из журнала регистрации событий в информационной системе персональных данных комиссия передает их в общий отдел для последующего хранения. Акты и выгрузки из журнала хранятся в течение трех лет с момента уничтожения персональных данных.

4.1.3. Ведение кадрового и бухгалтерского учета :

4.1.3.1. Категории и перечни персональных данных:

- вид, серия, номер документа, удостоверяющего личность, наименование органа, выдавшего его, дата выдачи;

- страховой номер индивидуального лицевого счета (СНИЛС);

- идентификационный номер налогоплательщика (ИНН);

- адрес и дата регистрации по месту жительства (место пребывания), адрес фактического проживания;
- номер контактного телефона, адрес электронной почты и (или) сведения о других способах связи;
- реквизиты свидетельств о государственной регистрации актов гражданского состояния и содержащиеся в них сведения;
- сведения о семейном положении, составе семьи (степень родства, фамилии, имена, отчества (при наличии), даты (число, месяц, год) и места рождения);
- сведения об образовании и (или) квалификации или наличии специальных знаний (в том числе наименование образовательной и (или) иной организации, год окончания, уровень образования, квалификация, реквизиты документа об образовании, обучении);
- сведения об отношении к воинской обязанности, о воинском учете и реквизиты документов воинского учета (серия, номер, дата выдачи документа, наименование органа, выдавшего его);
- сведения о трудовой деятельности, а также информация о предыдущих местах работы, периодах и стаже работы;
- сведения, содержащиеся в документах, дающих право на пребывание и трудовую деятельность на территории РФ (для иностранных граждан, пребывающих в РФ);
- сведения о доходах, обязательствах по исполнительным документам;
- номера расчетного счета, банковской карты

При оформлении работника отделом кадров формируется личное дело работника, в которое входит:

- заявления (прием, перевод, увольнение, о предоставлении отпуска по беременности и родам, о предоставлении отпусках по уходу за ребенком)
 - копии приказов (о предоставлении отпуска по беременности и родам, о предоставлении отпуска по уходу за ребенком и т. д.);
 - трудовой договор;
 - дополнительные соглашения к трудовому договору;
 - договор о материальной ответственности (при необходимости);
 - согласие на обработку персональных данных;
 - согласие на использование изображения;
- 4.1.3.2. Категории субъектов персональных данных.
- работники Оператора;
 - бывшие работники Оператора;
 - члены семей работников Оператора- в случаях, когда согласно законодательству сведения о них предоставляются работником.
- 4.1.3.3. Способы обработки персональных данных:
- автоматизированный и неавтоматизированный.
- 4.1.3.4.Сроки обработки и хранения данных:
- 50 лет .

4.1.3.5. Порядок уничтожения.

4.1.3.5.1. Уничтожение персональных данных осуществляет комиссия, созданная приказом директора.

4.1.3.5.2. . Комиссия составляет список с указанием документов, иных материальных носителей и (или) сведений в информационных системах, содержащих персональные данные, которые подлежат уничтожению.

4.1.3.5.3 Персональные данные на бумажных носителях уничтожаются с использованием shreddera. Персональные данные на электронных носителях уничтожаются путем механического нарушения целостности носителя, не позволяющего считать или восстановить персональные данные, а также путем удаления данных с электронных носителей методами и средствами гарантированного удаления остаточной информации.

4.1.3.5.4. Комиссия подтверждает уничтожение персональных данных, указанных в п.п. 4.1.3.1. Политики, согласно Требованиям к подтверждению уничтожения персональных данных, утвержденных Приказом Роскомнадзора от 28.10.2022 № 179, а именно:

- актом об уничтожении персональных данных- если данные обрабатываются без использования средств автоматизации;

- актом об уничтожении персональных данных и выгрузкой из журнала регистрации событий в информационной системе персональных данных- если данные обрабатываются с использованием средств автоматизации либо одновременно с использованием и без использования таких средств.

Акт может составляться на бумажном носителе или в электронной форме, подписанной электронными подписями.

Формы акта и выгрузки из журнала с учетом сведений, который должны содержаться в указанных документах, утверждаются приказом директора.

4.1.3.5.5. После составления акта об уничтожении персональных данных и выгрузки из журнала регистрации событий в информационной системе персональных данных комиссия передает их в общий отдел для последующего хранения. Акты и выгрузки из журнала хранятся в течение трех лет с момента уничтожения персональных данных.

4.1.4. Содействие работникам в получении образования и продвижения по службе.

4.1.4.1. Категории и перечни персональных данных

- фамилия, имя, отчество(при наличии), а также прежние фамилия, имя, отчество (при наличии);

- пол;

- дата (число, месяц, год) и место рождения;

- сведения о гражданстве;

- вид, серия, номер документа, удостоверяющего личность, наименование органа, выдавшего его, дата выдачи;

- страховой номер индивидуального лицевого счета (СНИЛС);

- идентификационный номер налогоплательщика (ИНН);

- адрес и дата регистрации по месту жительства (место пребывания), адрес фактического проживания;

- номер контактного телефона, адрес электронной почты и (или) сведения о других способах связи;

- реквизиты свидетельств о государственной регистрации актов гражданского состояния и содержащиеся в них сведения;

- сведения о семейном положении, составе семьи (степень родства, фамилии, имена, отчества (при наличии), даты (число, месяц, год) и места рождения);

- сведения об образовании и (или) квалификации или наличии специальных знаний (в том числе наименование образовательной и (или) иной организации, год окончания, уровень образования, квалификация, реквизиты документа об образовании, обучении);

- сведения об отношении к воинской обязанности, о воинском учете и реквизиты документов воинского учета (серия, номер, дата выдачи документа, наименование органа, выдавшего его);

- сведения о трудовой деятельности, а также информация о предыдущих местах работы, периодах и стаже работы;

- сведения, содержащиеся в документах, дающих право на пребывание и трудовую деятельность на территории РФ (для иностранных граждан, пребывающих в РФ);

4.1.4.2. . Категории субъектов персональных данных

- работники Оператора;

4.1.4.3. Способы обработки персональных данных:

- автоматизированный и неавтоматизированный

4.1.3.4.Сроки обработки и хранения данных:

- при достижении цели их обработки.

4.1.4.5. Порядок уничтожения.

4.1.4.5.1. Уничтожение персональных данных осуществляет комиссия, созданная приказом директора.

4.1.4.5.2. Комиссия составляет список с указанием документов, иных материальных носителей и (или) сведений в информационных системах, содержащих персональные данные, которые подлежат уничтожению.

4.1.4.5.3 Персональные данные на бумажных носителях уничтожаются с использованием shreddera. Персональные данные на электронных носителях уничтожаются путем механического нарушения целостности носителя, не позволяющего считать или восстановить персональные данные, а также путем удаления данных с электронных носителей методами и средствами гарантированного удаления остаточной информации.

4.1.4.5.4. Комиссия подтверждает уничтожение персональных данных, указанных в п.п. 4.1.4.1. Политики, согласно Требованиям к подтверждению уничтожения персональных данных, утвержденных Приказом Роскомнадзора от 28.10.2022 № 179, а именно:

- актом об уничтожении персональных данных- если данные обрабатываются без использования средств автоматизации;

- актом об уничтожении персональных данных и выгрузкой из журнала регистрации событий в информационной системе персональных данных- если данные обрабатываются с использованием средств автоматизации либо одновременно с использованием и без использования таких средств.

Акт может составляться на бумажном носителе или в электронной форме, подписанной электронными подписями.

Формы акта и выгрузки из журнала с учетом сведений, который должны содержаться в указанных документах, утверждаются приказом директора.

4.1.4.5.5. После составления акта об уничтожении персональных данных и выгрузки из журнала регистрации событий в информационной системе персональных данных комиссия передает их в общий отдел для последующего хранения. Акты и выгрузки из журнала хранятся в течение трех лет с момента уничтожения персональных данных.

4.1.5. Оформление наградений и поощрений

4.1.5.1. Категории и перечни персональных данных

- фамилия, имя, отчество;

- данные относящиеся к трудовой функции
(должность)

4.1.5.2. Категории субъектов персональных данных

- работники Оператора.

4.1.5.3. Способы обработки персональных данных:

- автоматизированный и неавтоматизированный

4.1.5.4. Сроки обработки и хранения данных:

- при достижении цели их обработки.

4.1.5.5. Порядок уничтожения.

4.1.5.5.1. Уничтожение персональных данных осуществляет комиссия, созданная приказом директора.

4.1.5.5.2. Комиссия составляет список с указанием документов, иных материальных носителей и (или) сведений в информационных системах, содержащих персональные данные, которые подлежат уничтожению.

4.1.5.5.3 Персональные данные на бумажных носителях уничтожаются с использованием shreddera. Персональные данные на электронных носителях уничтожаются путем механического нарушения целостности носителя, не позволяющего считать или восстановить персональные данные, а также путем удаления данных с электронных носителей методами и средствами гарантированного удаления остаточной информации.

4.1.5.5.4. Комиссия подтверждает уничтожение персональных данных, указанных в п.п. 4.1.5.1. Политики, согласно Требованиям к подтверждению уничтожения персональных данных, утвержденных Приказом Роскомнадзора от 28.10.2022 № 179, а именно:

- актом об уничтожении персональных данных- если данные обрабатываются без использования средств автоматизации;

- актом об уничтожении персональных данных и выгрузкой из журнала регистрации событий в информационной системе персональных данных- если данные обрабатываются с использованием средств автоматизации либо одновременно с использованием и без использования таких средств.

Акт может составляться на бумажном носителе или в электронной форме, подписанной электронными подписями.

Формы акта и выгрузки из журнала с учетом сведений, который должны содержаться в указанных документах, утверждаются приказом директора.

4.1.5.5. После составления акта об уничтожении персональных данных и выгрузки из журнала регистрации событий в информационной системе персональных данных комиссия передает их в общий отдел для последующего хранения. Акты и выгрузки из журнала хранятся в течение трех лет с момента уничтожения персональных данных.

4.1.6. Предоставление со стороны Оператора установленных законодательством условий труда, гарантий и компенсаций.

4.1.6.1. . Категории и перечни персональных данных:

- вид, серия, номер документа, удостоверяющего личность, наименование органа, выдавшего его, дата выдачи;

- страховой номер индивидуального лицевого счета (СНИЛС);

- идентификационный номер налогоплательщика (ИНН);

4.1.6.2. Категории субъектов персональных данных.

- работники Оператора;

- бывшие работники Оператора;

- члены семей работников Оператора- в случаях, когда согласно законодательству сведения о них предоставляются работником.

4.1.6.3. Способы обработки персональных данных:

- автоматизированный и неавтоматизированный

4.1.6.4. Сроки обработки и хранения данных:

- при достижении цели их обработки

4.1.6.5. Порядок уничтожения.

4.1.6.5.1. Уничтожение персональных данных осуществляет комиссия, созданная приказом директора.

4.1.6.5.2. . Комиссия составляет список с указанием документов, иных материальных носителей и (или) сведений в информационных системах, содержащих персональные данные, которые подлежат уничтожению.

4.1.6.5.3 Персональные данные на бумажных носителях уничтожаются с использованием shreddera. Персональные данные на электронных носителях уничтожаются путем механического нарушения целостности носителя, не позволяющего считать или восстановить персональные данные, а также путем удаления данных с электронных носителей методами и средствами гарантированного удаления остаточной информации.

4.1.6.5.4. Комиссия подтверждает уничтожение персональных данных, указанных в п.п. 4.1.6.1. Политики, согласно Требованиям к подтверждению уничтожения персональных данных, утвержденных Приказом Роскомнадзора от 28.10.2022 № 179, а именно:

- актом об уничтожении персональных данных- если данные обрабатываются без использования средств автоматизации;

- актом об уничтожении персональных данных и выгрузкой из журнала регистрации событий в информационной системе персональных данных- если данных обрабатываются с использованием средств автоматизации либо одновременно с использованием и без использования таких средств.

Акт может составляться на бумажном носителе или в электронной форме, подписанной электронными подписями.

Формы акта и выгрузки из журнала с учетом сведений, который должны содержаться в указанных документах, утверждаются приказом директора.

4.1.6.5.5. После составления акта об уничтожении персональных данных и выгрузки из журнала регистрации событий в информационной системе персональных данных комиссия

передает их в общий отдел для последующего хранения. Акты и выгрузки из журнала хранятся в течение трех лет с момента уничтожения персональных данных.

4.1.7. Оказание медицинских услуг, в том числе идентификации пациентов (заказчиков), отражения информации в медицинской документации.

4.1.7.1. Категории и перечни персональных данных:

- фамилия, имя, отчество;
- пол;
- возраст;
- дата рождения;
- вид, серия, номер документа, удостоверяющего личность, наименование органа, выдавшего его, дата выдачи;
- страховой номер индивидуального лицевого счета (СНИЛС);
- адрес и дата регистрации по месту жительства (место пребывания), адрес фактического проживания;
- номер контактного телефона, адрес электронной почты и (или) сведения о других способах связи;
- сведения о семейном положении, составе семьи (степень родства, фамилии, имена, отчества (при наличии), даты (число, месяц, год) и места рождения);
- данные о состоянии здоровья, в том числе биометрические персональные данные (рост, вес, телосложение);
- сведения о наличии льгот;
- сведения о степени родства с пациентом;
- сведения о документе, дающем право на представление интересов пациента.

4.1.7.2. Категории субъектов персональных данных

- Пациенты, законные представители пациентов;

4.1.7.3. Способы обработки персональных данных:

- автоматизированный и неавтоматизированный.

4.1.7.4. Сроки обработки и хранения данных:

- при достижении цели их обработки.

4.1.7.5. . Порядок уничтожения.

4.1.7.5.1. Уничтожение персональных данных осуществляет комиссия, созданная приказом директора.

4.1.7.5.2. . Комиссия составляет список с указанием документов, иных материальных носителей и (или) сведений в информационных системах, содержащих персональные данные, которые подлежат уничтожению.

4.1.7.5.3 Персональные данные на бумажных носителях уничтожаются с использованием shreddera. Персональные данные на электронных носителях уничтожаются путем механического нарушения целостности носителя, не позволяющего считать или восстановить персональные данные, а также путем удаления данных с электронных носителей методами и средствами гарантированного удаления остаточной информации.

4.1.7.5.4. Комиссия подтверждает уничтожение персональных данных, указанных в п.п.

4.1.7.1. Политики, согласно Требованиям к подтверждению уничтожения персональных данных, утвержденных Приказом Роскомнадзора от 28.10.2022 № 179, а именно:

- актом об уничтожении персональных данных- если данные обрабатываются без использования средств автоматизации;
- актом об уничтожении персональных данных и выгрузкой из журнала регистрации событий в информационной системе персональных данных- если данных обрабатываются с использованием средств автоматизации либо одновременно с использованием и без использования таких средств.

Акт может составляться на бумажном носителе или в электронной форме, подписанной электронными подписями.

Формы акта и выгрузки из журнала с учетом сведений, который должны содержаться в указанных документах, утверждаются приказом директора.

4.1.7.5.5. После составления акта об уничтожении персональных данных и выгрузки из журнала регистрации событий в информационной системе персональных данных комиссия передает их в общий отдел для последующего хранения. Акты и выгрузки из журнала хранятся в течение трех лет с момента уничтожения персональных данных.

4.1.8. Предоставление сведений страховым компаниям (в случае оплаты пациентов оказываемых услуг).

4.1.8.1. Категории и перечни персональных данных:

- фамилия, имя, отчество;
- пол;
- возраст;
- дата рождения;
- вид, серия, номер документа, удостоверяющего личность, наименование органа, выдавшего его, дата выдачи;
- страховой номер индивидуального лицевого счета (СНИЛС);
- адрес и дата регистрации по месту жительства (место пребывания), адрес фактического проживания;
- номер контактного телефона, адрес электронной почты и (или) сведения о других способах связи;
- сведения о семейном положении, составе семьи (степень родства, фамилии, имена, отчества (при наличии), даты (число, месяц, год) и места рождения);
- данные о состоянии здоровья, в том числе биометрические персональные данные (рост, вес, телосложение);
- сведения о наличии льгот;
- сведения о степени родства с пациентом;
- сведения о документе, дающем право на представление интересов пациента.

4.1.8.2. Категории субъектов персональных данных

- Пациенты, законные представители пациентов;

4.1.8.3. Способы обработки персональных данных:

- автоматизированный и неавтоматизированный.

4.1.8.4. Сроки обработки и хранения данных:

- при достижении цели их обработки.

4.1.8.5. Порядок уничтожения.

4.1.8.5.1. Уничтожение персональных данных осуществляет комиссия, созданная приказом директора.

4.1.8.5.2. Комиссия составляет список с указанием документов, иных материальных носителей и (или) сведений в информационных системах, содержащих персональные данные, которые подлежат уничтожению.

4.1.8.5.3 Персональные данные на бумажных носителях уничтожаются с использованием shreddera. Персональные данные на электронных носителях уничтожаются путем механического нарушения целостности носителя, не позволяющего считать или восстановить персональные данные, а также путем удаления данных с электронных носителей методами и средствами гарантированного удаления остаточной информации.

4.1.8.5.4. Комиссия подтверждает уничтожение персональных данных, указанных в п.п. 4.1.8.1. Политики, согласно Требованиям к подтверждению уничтожения персональных данных, утвержденных Приказом Роскомнадзора от 28.10.2022 № 179, а именно:

- актом об уничтожении персональных данных- если данные обрабатываются без использования средств автоматизации;
- актом об уничтожении персональных данных и выгрузкой из журнала регистрации событий в информационной системе персональных данных- если данных обрабатываются с использованием средств автоматизации либо одновременно с использованием и без использования таких средств.

Акт может составляться на бумажном носителе или в электронной форме, подписанной электронными подписями.

Формы акта и выгрузки из журнала с учетом сведений, который должны содержаться в указанных документах, утверждаются приказом директора.

4.1.8.5.5. После составления акта об уничтожении персональных данных и выгрузки из журнала регистрации событий в информационной системе персональных данных комиссия передает их в общий отдел для последующего хранения. Акты и выгрузки из журнала хранятся в течение трех лет с момента уничтожения персональных данных.

4.1.9. Предоставление отчетности в отношении оказанных медицинских услуг.

4.1.9.1. Категории и перечни персональных данных:

- фамилия, имя, отчество;
- пол;
- возраст;
- дата рождения;
- вид, серия, номер документа, удостоверяющего личность, наименование органа, выдавшего его, дата выдачи;
- страховой номер индивидуального лицевого счета (СНИЛС);
- адрес и дата регистрации по месту жительства (место пребывания), адрес фактического проживания;
- номер контактного телефона, адрес электронной почты и (или) сведения о других способах связи;
- сведения о семейном положении, составе семьи (степень родства, фамилии, имена, отчества (при наличии), даты (число, месяц, год) и места рождения);
- данные о состоянии здоровья, в том числе биометрические персональные данные (рост, вес, телосложение);
- сведения о наличии льгот;
- сведения о степени родства с пациентом;
- сведения о документе, дающем право на представление интересов пациента.

4.1.9.2. Категории субъектов персональных данных

- Пациенты, законные представители пациентов;

4.1.9.3. Способы обработки персональных данных:

- автоматизированный и неавтоматизированный.

4.1.9.4. Сроки обработки и хранения данных:

- при достижении цели их обработки.

4.1.9.5. . Порядок уничтожения.

4.1.9.5.1. Уничтожение персональных данных осуществляет комиссия, созданная приказом директора.

4.1.9.5.2. Комиссия составляет список с указанием документов, иных материальных носителей и (или) сведений в информационных системах, содержащих персональные данные, которые подлежат уничтожению.

4.1.9.5.3 Персональные данные на бумажных носителях уничтожаются с использованием shreddera. Персональные данные на электронных носителях уничтожаются путем механического нарушения целостности носителя, не позволяющего считать или восстановить персональные данные, а также путем удаления данных с электронных носителей методами и средствами гарантированного удаления остаточной информации.

4.1.9.5.4. Комиссия подтверждает уничтожение персональных данных, указанных в п.п. 4.1.9.1. Политики, согласно Требованиям к подтверждению уничтожения персональных данных, утвержденных Приказом Роскомнадзора от 28.10.2022 № 179, а именно:

- актом об уничтожении персональных данных- если данные обрабатываются без использования средств автоматизации;

- актом об уничтожении персональных данных и выгрузкой из журнала регистрации событий в информационной системе персональных данных- если данных обрабатываются с использованием средств автоматизации либо одновременно с использованием и без использования таких средств.

Акт может составляться на бумажном носителе или в электронной форме, подписанной электронными подписями.

Формы акта и выгрузки из журнала с учетом сведений, который должны содержаться в указанных документах, утверждаются приказом директора.

4.1.9.5.5. После составления акта об уничтожении персональных данных и выгрузки из журнала регистрации событий в информационной системе персональных данных комиссия передает их в общий отдел для последующего хранения. Акты и выгрузки из журнала хранятся в течение трех лет с момента уничтожения персональных данных.

5. Правовые основания обработки персональных данных.

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

5.2. Оператор обрабатывает персональные данные на основании:

Трудового кодекса Российской Федерации;

Федерального закона «Об основах охраны здоровья граждан в Российской Федерации» и принятых на его основе нормативно-правовых актов, регулирующих отношения, связанные с оказанием медицинских услуг;

иных федеральных законов и прочих нормативных правовых актов;

устава Оператора;

договоров, заключаемых между Оператором и субъектами персональных данных;

согласий на обработку персональных данных.

6. Основные права и обязанности Оператора персональных данных.

6.1. Оператор при сборе персональных данных обязан предоставить субъекту персональных данных по его просьбе информацию, касающуюся обработки его персональных данных:

6.2. Если предоставление персональных данных является обязательным в соответствии с федеральным законом, Оператор обязан разъяснить субъекту персональных данных юридические последствия отказа предоставить его персональные данные.

6.3. При сборе персональных данных, в том числе посредством информационно-телекоммуникационной сети интернет, Оператор обязан обеспечить 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 Федеральном законе «О персональных данных»

6.4. Оператор обязан принимать меры, необходимые и достаточные для обеспечения выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами.

6.5. Оператор обязан опубликовать или иным образом обеспечить неограниченный доступ к настоящей Политике, к сведениям о реализуемых требованиях к защите персональных данных. Оператор в случае осуществления сбора персональных данных с использованием информационно-телекоммуникационных сетей обязан опубликовать в соответствующей информационно-телекоммуникационной сети Политику и сведения о реализуемых требованиях к защите персональных данных, а также обеспечить возможность доступа к указанному документу с использованием соответствующей информационно-телекоммуникационной сети.

6.6. Оператор при обработке персональных данных обязан 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.

6.7. Оператор обязан предоставлять субъекту персональных данных информацию о том, какие данные о нем он будет обрабатывать, если эти персональные данные о нем он будет обрабатывать, если эти персональные данные получены не от субъекта персональных данных.

6.8. Обеспечивать взаимодействие с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак (ГосСОПКА) и информировать

6.9. Оператор вправе поручать обработку персональных данных другому лицу с согласия субъекта персональных данных, если иное не предусмотрено федеральным законом, на основании заключаемого с этим лицом договора. Лицо, осуществляющее обработку персональных данных по поручению Оператора, обязано соблюдать принципы и правила обработки персональных данных, предусмотренные Федеральным законом «О персональных данных». В поручении Оператора должны быть определены перечень действий (операций) с персональными данными, которые будут совершаться лицом, осуществляющим обработку персональных данных, и цели обработки, должна быть установлена обязанность такого лица соблюдать конфиденциальность и обеспечивать безопасность персональных данных при их обработке, а также должны быть указаны требования к защите обрабатываемых персональных данных в соответствии со статьей 19 Федерального закона «О персональных данных».

6.10. Оператор обязан предоставлять субъекту ПД информацию о том, какие данные о нем он будет обрабатывать, если эти ПД получены не от субъекта ПД.

6.11. Оператор обязан обеспечивать взаимодействие с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак (ГосСОПКА) и информировать Роскомнадзор о компьютерных инцидентах, повлекших неправомерную передачу (предоставление, распространение, доступ) ПД.

6.12. Оператор обязан уведомлять Роскомнадзор в течение 24 часов о факте неправомерной или случайной передачи ПД, повлекшей нарушение прав субъектов ПД, а также о предполагаемых причинах и вреде, нанесенном правом субъектов ПД, о принятых мерах по устранению последствий инцидента.

6.13. Оператор обязан в течение 72 часов уведомлять Роскомнадзор о результатах внутреннего расследования по поводу инцидента и сообщать о лицах, действие которых стали причиной утечки ПД.

7. Основные права и обязанности субъекта персональных данных.

7.1. 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.

7.2. Обработка персональных данных в целях продвижения товаров, работ, услуг на рынке путем осуществления прямых контактов с потенциальным потребителем с помощью средств связи, допускается только при условии предварительного согласия субъекта персональных данных.

7.3. Принятие 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 разрешается только при наличии согласия в письменной форме субъекта персональных данных или в случаях, предусмотренных федеральными законами, устанавливающими также меры по обеспечению соблюдения прав и законных интересов субъекта персональных данных.

7.4. Если субъект персональных данных считает, что Оператор осуществляет обработку его персональных данных с нарушением требований Федерального закона «О персональных данных» или иным образом нарушает его права и свободы, субъект персональных данных

вправе обжаловать действия или бездействия Оператора в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке.

7.5. 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.

8. Порядок и условия обработки персональных данных.

8.1. Обработка персональных данных осуществляется после принятия необходимых мер по защите персональных данных.

8.2. Оператор не вправе обрабатывать персональные данные субъекта персональных данных без его письменного согласия, за исключением случаев, предусмотренных статьей 6 Федерального закона «О персональных данных».

8.3. Письменное согласие субъекта персональных данных должно включать:

фамилию, имя, отчество;

адрес субъекта персональных данных;

номер основного документа, удостоверяющего личность, сведения о дате выдачи указанного документа и выдавшем его органе;

наименование и адрес Оператора;

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;

способ его отзыва;

подпись субъекта персональных данных

Для удобства субъектов, а также контроля учета требований законодательства, допускается включение согласия в типовые формы (бланки) согласий и в договоры с субъектами персональных данных.

8.4. Оператор организует обработку персональных данных в следующем порядке:

8.4.1. Назначает ответственное лицо за организацию обработки персональных данных, устанавливает перечень лиц, имеющих доступ к персональным данным

8.4.2. Издаёт настоящую Политику, локальные акты по вопросам обработки персональных данных;

8.4.3. Применяет правовые, организационные и технические меры по обеспечению безопасности персональных данных;

8.4.4. Осуществляет внутренний контроль, за соответствием обработки персональных данных Федеральному закону «О персональных данных» и принятым в соответствии с ним нормативным правовым актам, требованиям к защите персональных данных, настоящей Политике, локальным актам Оператора;

8.4.5. Осуществляет оценку вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона «О персональных данных», определяет соотношение указанного вреда и принимаемых оператором мер, направленных на обеспечение выполнения обязанностей, предусмотренных данным Федеральным законом;

8.4.6. Знакомит работников Оператора, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, в том числе с требованиями к защите персональных данных, настоящей Политики, локальными актами по вопросам обработки персональных данных, и (или) обучение указанных работников.

8.5. Оператор при обработке персональных данных принимает необходимые правовые, организационные и технические меры, в том числе:

8.5.1. Определяет угрозы безопасности персональных данных при их обработке в информационных системах персональных данных;

8.5.2. Применяет организационные и технические меры по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, необходимые для выполнения требований к защите персональных данных.

8.5.3. Оценивают эффективность принимаемых мер по обеспечению безопасности персональных данных;

8.5.4. Учитывает машинные носители персональных данных;

8.5.5. Обнаруживает факты несанкционированного доступа к персональным данным и принимает меры;

8.5.6. Восстанавливает персональные данные, модифицированные или уничтоженные вследствие несанкционированного доступа к ним;

8.5.7. Устанавливает правила доступа к персональным данным, обрабатываемым в информационной системе персональных данных, а также обеспечивает регистрацию и учет всех действий, совершаемых с персональными данными в информационной системе персональных данных.

8.6. При обработке персональных данных Оператор выполняет, в частности, сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

8.7. Хранение персональных данных Субъектов осуществляется следующими способами:
в бумажном виде;

на электронных носителях автоматизированных рабочих мест;

в информационных системах Оператора.

8.8. Персональные данные Субъекта, представленные в бумажном виде, хранятся в помещениях Оператора. Материальные носители, представленные в бумажном виде, хранятся в сейфе, в запираемом металлическом шкафу или помещении, исключающим несанкционированный доступ.

8.9. Персональные данные, обрабатываемые в информационных системах, хранятся в базах данных, располагающихся в помещениях Оператора, исключающих несанкционированный доступ.

8.10. В целях обеспечения сохранности и конфиденциальности персональных данных все операции с персональными данными выполняются только работниками Оператора, осуществляющими данную работу в соответствии с трудовыми обязанностями. Оператором введен режим ограниченного доступа к персональным данным.

8.11. Оператором реализована разрешительная система доступа (матрица доступа) к информационным (программным) ресурсам в информационных системах ПДн Оператора.

8.12. Оператор получает персональные данные непосредственно от субъектов персональных данных или их представителей, наделенных соответствующими полномочиями. Согласия субъекта на получение его персональных данных от третьих лиц не требуется в случаях, когда согласие субъекта на передачу его персональных данных третьим лицам получено от него в письменном виде при заключении договора с Оператором, а также в случаях, установленных федеральным законом.

8.12.1. Оператор вправе передавать персональные данные органам дознания и следствия, иным уполномоченным органам по основаниям, предусмотренным действующим законодательством.

8.12.2. При передаче персональных данных третьим лицам для исполнения обязательств по договорам с субъектом персональных данных, от третьих лиц берут на себя обязательства по обеспечению безопасности полученных ими персональных данных и сохранения конфиденциальности.

8.13. Работникам Оператора запрещается хранение документов с персональными данными и их копий на рабочих местах и (или) в открытом доступе, оставлять шкафы (сейфы) открытыми в случае выхода работника из рабочего помещения.

8.14. Работникам запрещено устанавливать постороннее программное обеспечение на машинные носители, подключать личные мобильные устройства и носители информации.

8.15. Работникам запрещено разглашать конфиденциальную информацию, которая стала им известна при работе с информационными системами Оператора третьим лицам.

8.16. В электронном виде документы, содержащие персональные данные, хранятся в обезличенном состоянии в специализированных базах данных с ограниченным правом доступа. Базы данных находятся в охраняемых помещениях с ограниченными правами доступа.

8.17. При увольнении работника, имеющего доступ к персональным данным, прекращении доступа к персональным данным, документы и иные носители, содержащие персональные данные, сдаются работником своему непосредственному руководителю.

8.18. В случае выявления нарушений порядка обработки персональных данных уполномоченными работниками незамедлительно принимаются меры по установлению причин нарушений и их устранению.

8.19. В состав мер по обеспечению безопасности персональных данных, реализуемых в рамках системы защиты персональных данных с учетом актуальных угроз безопасности персональных данных и применяемых информационных технологий, входят:

- идентификация и аутентификация субъектов доступа и объектов доступа;
- разграничение уровней субъектов доступа к объектам доступа;
- ограничение программной среды;
- защита машинных носителей информации, на которых хранятся персональные данные;
- регистрация событий безопасности;
- антивирусная защита для машин пользователей и серверов;
- средства межсетевое экранирования;
- обнаружение (предотвращение) вторжений;
- контроль (анализ) защищенности персональных данных;
- обеспечение целостности информационной системы и персональных данных;
- выявление инцидентов (одного события или группы событий), которые могут привести к сбоям или нарушению функционирования информационной системы и (или) к возникновению угроз безопасности персональных данных, и реагирование на них;
- управление конфигурацией информационной системы защиты персональных данных.

8.20. Под актуальными угрозами безопасности персональных данных понимается совокупность условий и факторов, создающих актуальную опасность несанкционированного, в том числе случайного, доступа к персональным данным при их обработке в информационной системе, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия.

8.21. Определение типа угроз безопасности персональных данных, актуальных для информационной системы, производится с учетом оценки возможного вреда, проведенной во исполнение пункта 5 части 1 статьи 18.1 Федерального закона «О персональных данных».

8.22. Организация и контроль за выполнением указанных мероприятий возлагается на лица, ответственные за организацию обработки и защиты ПДн в Организации. Разрабатываемые документы подлежат утверждению руководителем Организации. Размещение информационных систем, специальное оборудование и охрана помещений, в которых ведется работа с персональными данными, организация режима обеспечения безопасности в этих помещениях обеспечивает сохранность носителей ПДн, а также исключает возможность неконтролируемого проникновения или пребывания в этих помещениях посторонних лиц.

8.23. Требования к помещениям, в которых производится обработка ПДн, а также к порядку предоставления доступа в эти помещения, охране и режиму физической безопасности в целом определяются в Положении о внутриобъектовом режиме.

8.24. Условием прекращения обработки персональных данных может являться достижение целей обработки персональных данных, истечение срока действия согласия на обработку персональных данных или отзыв согласия субъектом персональных данных, по достижению предельных сроков хранения документации, предусмотренных действующим законодательством.

8.25. Оператор обрабатывает персональные данные уволенных сотрудников в случаях и сроки, предусмотренные действующим законодательством (с учетом Приказа Минкультуры России от 25.08.2010 № 558 «Об утверждении «Перечня типовых управленческих архивных документов, образующихся в процессе деятельности государственных органов, органов местного самоуправления и организаций, с указанием сроков хранения»)

8.25.1. При ликвидации Оператора, документы по личному составу, а также архивные документы, сроки временного хранения которых не истекли, в упорядоченном состоянии поступают на хранение в соответствующий государственный или муниципальный архив.

8.25.2. При реорганизации Оператора архивные документы в упорядоченном состоянии передаются правопреемнику Оператора.

8.26. Оператор обрабатывает персональные данные пациентов, в сроки предусмотренные Минздравом России (Письмо от 07.12.2015 № 13-2/1538 «О сроках хранения медицинской документации»).

9. Актуализация, исправление, удаление персональных данных, ответы на запросы субъектов на доступ к персональным данным.

9.1. 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 персональные данные на основании договора с Оператором или на основании Федерального закона;

обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок предоставления таких данных не предусмотрен федеральным законом;

сроки обработки персональных данных, в том числе сроки их хранения;

порядок осуществления субъектом персональных данных прав, предусмотренных Федеральным законом «О персональных данных»;

информацию об осуществленной или предполагаемой трансграничной передаче данных;

наименование или фамилию, имя, отчество и адрес, осуществляющего обработку персональных данных по поручению Оператора, если обработка поручена или будет поручена такому лицу;

иные сведения, предусмотренные Федеральным законом «О персональных данных» или другими федеральными законами.

9.2. Указанные выше сведения должны быть предоставлены субъекту 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.

9.3. Сведения, указанные в пункте 9.1, предоставляются субъекту персональных данных или его представителю Оператором при обращении либо при получении запроса субъекта персональных данных или его представителя. Запрос 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 карты амбулаторного больного), либо сведения, иным образом подтверждающие факт обработки персональных данных Оператором, подпись субъекта персональных данных или его представителя.

9.4. В случае, если сведения, указанные в пункте 9.1, а также обрабатываемые персональные данные были предоставлены для ознакомления субъекту персональных данных по его запросу, субъект персональных данных вправе обратиться повторно к Оператору или направить ему повторный запрос в целях получения сведений, указанных в пункте 9.1, и

ознакомления с такими персональными данными не ранее чем 30 дней после первоначального обращения или направления первоначального запроса, если более короткий срок не установлен федеральным законом, принятым в соответствии с ним нормативным правовым актом или договором, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных.

9.5. Субъект персональных данных вправе обратиться повторно к Оператору или направить ему повторный запрос в целях получения сведений, указанных в пункте 9.1, а также в целях ознакомления с обрабатываемыми персональными данными до истечения срока, указанного в пункте 9.4., в случае, если такие сведения и (или) обрабатываемые персональные данные не были предоставлены ему ознакомления в полном объеме по результатам рассмотрения первоначального обращения. Повторный запрос наряду со сведениями, указанными в пункте 9.1, должен содержать обоснование направления повторного запроса.

9.6. В течении 10 рабочих дней, считая с момента обращения получения запроса Оператор должен:

9.6.1. Предоставить субъекту персональных данных информацию, касающуюся обработки его персональных данных.

9.6.2. Предоставить возможность субъекту ознакомиться с его персональными данными, находящимися у Оператора, либо дать письменный отказ в предоставлении такой информации.

9.6.3. Предоставить в Роскомнадзор запрошенные этим органом сведения.

9.6.4. Прекратить обработку персональных данных по требованию субъекта персональных данных.

9.7. Оператор обязан предоставить безвозмездно субъекту персональных данных или его представителю возможность ознакомления с персональными данными, относящимися к этому субъекту персональных данных.

9.9. В срок, не превышающий семи рабочих дней со дня предоставления субъектом персональных данных или его представителем сведений, подтверждающих, что персональные данные являются неполными, неточными или неактуальными, Оператор обязан внести в них необходимые изменения.

9.10. В срок, не превышающий семи рабочих дней со дня представления субъектом персональных данных или его представителем сведений, подтверждающих, что такие персональные данные являются незаконно полученными или не являются необходимыми для заявленной цели обработки, Оператор обязан уничтожить такие персональные данные.

9.11. Оператор обязан уведомить субъекта персональных данных или его представителя о внесенных изменениях и предпринятых мерах и принять разумные меры для уведомления третьих лиц, которым персональные данные этого субъекта были переданы.

9.12. В случае выявления неправомерной обработки персональных данных при обращении субъекта персональных данных или его представителя, либо по запросу субъекта персональных данных или его представителя, либо уполномоченного органа по защите прав субъектов персональных данных Оператор обязан осуществить блокирование неправомерно обрабатываемых персональных данных, относящихся к этому субъекту персональных данных, или обеспечить их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению Оператора) с момента такого обращения или получения указанного запроса на период проверки.

9.13. В случае выявления неточных персональных данных при обращении субъекта персональных данных или его представителя либо по их запросу или по запросу уполномоченного органа по защите прав субъектов персональных данных Оператор обязан осуществить блокирование персональных данных, относящихся к этому субъекту персональных данных, или обеспечить 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.

9.14. 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.

9.15. В случае выявления неправомерной обработки персональных данных, осуществляемой Оператором или лицом, действующим по поручению Оператора, Оператор в срок, не превышающий трех рабочих дней с даты этого выявления, обязан прекратить неправомерную обработку персональных данных ил 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 10 рабочих дней с даты выявления неправомерной обработки персональных данных, обязан уничтожить такие персональные данные или обеспечить их уничтожение. Об устранении допущенных нарушений или об уничтожении персональных данных Оператор обязан уведомить субъекта персональных данных или его представителей, а в случае, если обращение субъекта персональных данных или его представителя либо запрос уполномоченного органа по защите прав субъектов персональных данных были направлены уполномоченным органом по защите прав субъектов персональных данных, также указанный орган.

10. Ответственность за нарушение правил обработки и защиты персональных данных.

10.1. Лица, виновные в нарушении норм, регулирующих обработку и защиту ПДн, несут дисциплинарную, административную, гражданско- правовую и уголовную ответственность в соответствии с законодательством РФ.

10.2. Лица, имеющие доступ к персональным данным, несут персональную ответственность за несанкционированное распространение персональных данных, а также за соблюдение установленного в Организации порядка обеспечения безопасности в отношении персональных данных.

10.3. Руководитель подразделения, разрешающий доступ лиц к персональным данным, несет персональную ответственность за:

данное разрешение;

выполнение возложенных на него функций по организации обработки и защите персональных данных, обрабатываемых подразделением.

10.4. Каждое лицо, получающее для работы носитель информации, содержащий персональные данные, несет персональную ответственность за сохранность данного носителя.

10.5. Лица, в обязанность которых входит обработка персональных данных, обязаны обеспечить каждому субъекту персональных данных возможность ознакомления с документами и материалами, непосредственно затрагивающими его права и свободы, если иное не предусмотрено законодательством РФ. Неправомерный отказ в предоставлении собранных в установленном порядке документов, либо несвоевременное предоставление таких документов или иной информации в случаях, предусмотренных законом, либо предоставление законодательства в области ПДн- влекут за собой ответственность, предусмотренную действующим законодательством.

11. Конфиденциальность.

11.1. Организация и ее представители, получившие доступ к персональным данным, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия Субъекта персональных данных, если иное не предусмотрено федеральными законами.