

УТВЕРЖДАЮ:
Генеральный директор
ООО «А-СТОМ»

« 31/03 » 2026 г.

М.Ю. Юшков



ПОЛИТИКА
Общества с ограниченной ответственностью «А-СТОМ»
в отношении обработки персональных данных
(редакция 01._2026)

1. Общие положения

1.1. Настоящая Политика в отношении обработки персональных данных (далее – Политика) составлена в соответствии с пунктом 2 части 1 статьи 18.1 Федерального закона № 152-ФЗ от 27.07.2006г. «О персональных данных» и является основополагающим внутренним нормативно-правовым (локальным) документом Общества с ограниченной ответственностью «А-СТОМ» (далее – ООО «А-СТОМ»/ Организация/ Оператор), определяющим ключевые направления его деятельности в области обработки и защиты персональных данных.

1.2. Политика разработана во исполнение требований законодательства Российской Федерации в области обработки и защиты персональных данных (далее – ПДн) и направлена на обеспечение защиты прав и свобод человека и гражданина при обработке его ПДн в Организации, в том числе защиты прав на неприкосновенность частной жизни, личной, семейной, а также врачебной тайны.

1.3. Цель разработки и утверждения настоящей Политики – это определение порядка обработки и защиты персональных данных физических лиц: работников Организации, пациентов (клиентов) стоматологической клиники ООО «А-СТОМ», данные которых подлежат обработке, на основании полномочий медицинской организации; партнеров (контрагентов) Организации.

Политика действует в отношении всех персональных данных, которые обрабатывает ООО «А-СТОМ».

1.4. Во исполнение требований части 2 статьи 18.1 Федерального закона № 152-ФЗ от 27.07.2006 г. «О персональных данных» настоящая Политика публикуется в свободном доступе в информационно-телекоммуникационной сети Интернет на сайте Оператора и подлежит размещению в местах обслуживания пациентов медицинской организации ООО «А-СТОМ».

1.5. Правовым основанием обработки персональных данных в Организации является совокупность нормативных правовых актов, во исполнение которых и в соответствии с которыми Оператор осуществляет обработку персональных данных, в том числе с выполнением Организацией функций, предусмотренных учредительными документами, и определяемых:

- Конституцией Российской Федерации;
- Гражданским кодексом Российской Федерации;
- Трудовым кодексом Российской Федерации;
- Налоговым кодексом Российской Федерации;
- Федеральным законом № 152-ФЗ от 27.07. 2006 г. «О персональных данных» (в редакции от 24.06.2025 г.) (далее по тексту - Закон 152-ФЗ);
- Федеральным законом от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федеральным законом от 21.11.2011 г. № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации» (далее по тексту – Закон 323-ФЗ);
- Постановлением Правительства Российской Федерации от 1.09.2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;
- Постановлением Правительства РФ от 01.11.2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- Федеральным законом от 08.02.1998 г. № 14-ФЗ «Об обществах с ограниченной ответственностью»;

- Федеральным законом от 06.12.2011 г. № 402-ФЗ «О бухгалтерском учете»;
- Федеральным законом от 15.12.2001г. № 167-ФЗ «Об обязательном пенсионном страховании в Российской Федерации»;
- Приказом Роскомнадзора от 24.02.2021 г. № 18 «Об утверждении требований к содержанию согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения».
- иными нормативно правовыми актами, регулирующие отношения, связанные с деятельностью Оператора.

1.6. Правовым основанием обработки персональных данных также являются Устав Организации; договоры, заключаемые с Субъектом персональных данных; согласие Субъекта персональных данных на обработку его персональных данных.

1.7. Обработка ПДн в Организации осуществляется в ходе трудовых и иных непосредственно связанных с ними отношений, в которых Организация выступает в качестве работодателя (глава 14 Трудового кодекса Российской Федерации), в качестве исполнителя при оказании медицинских (стоматологических) услуг (статьи 13, 14, 78-79, 91-94 Закона № 323-ФЗ), а также в связи с реализацией Организацией своих прав и обязанностей как юридического лица.

1.8. Обработка персональных данных ограничивается достижением конкретных, заранее определенных и законных целей. Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных.

1.9. Обработке подлежат только персональные данные, которые отвечают целям их обработки.

1.10. Субъект персональных данных принимает решение о предоставлении его персональных данных и дает согласие на их обработку свободно, своей волей и в своем интересе.

Согласие на обработку персональных данных должно быть конкретным, предметным, информированным, сознательным и однозначным.

2. Основные термины и принятые сокращения

Персональные данные (ПДн) – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

Обработка персональных данных – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая в себя в том числе:

- сбор
- запись
- систематизация
- накопление
- хранение
- уточнение (обновление, изменение)
- извлечение
- использование
- передача (распространение, предоставление, доступ)
- блокирование
- удаление
- уничтожение персональных данных.

Оператор – государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

В рамках настоящей Политики **Оператором выступает ООО «А-СТОМ»** (ИНН 2801089879, ОГРН 1032800054913).

Распространение персональных данных – действия, направленные на раскрытие персональных данных неопределенному кругу лиц.

Предоставление персональных данных – действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц.

Блокировка персональных данных – временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных).

Уничтожение (ликвидация) персональных данных – действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе

персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных.

Автоматизированная обработка персональных данных – обработка персональных данных с помощью средств вычислительной техники.

Система персональных данных (ИСПД) – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

Конфиденциальность персональных данных - обязательное для соблюдения Оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространения без согласия субъекта персональных данных или наличия иного законного основания.

Материальный носитель персональных данных - материальный объект, используемый для закрепления и хранения информации. В целях настоящего Политики под материальным носителем понимается бумажный документ, диск, дискета, флэш-карта и т.п.

Работник – физическое лицо, с которым заключен трудовой договор или договор гражданско-правового характера.

Пациент – физическое лицо, которому оказывается медицинская помощь или которое обратилось за оказанием медицинской помощи независимо от наличия у него заболевания и от его состояния.

Медицинская деятельность – профессиональная деятельность Организации по оказанию медицинских (стоматологических) услуг на основании выданной лицензии.

Лечащий врач – специалисты медицинской организации ООО «А-СТОМ», на которых возложены функции по организации и непосредственному оказанию пациенту медицинской помощи (стоматологических услуг) в период наблюдения за ним и его лечения.

Цель обработки персональных данных - конкретный конечный результат действий, совершенных с персональными данными, вытекающий из требований законодательства и направленный, в том числе на создание необходимых правовых условий для достижения оптимального согласования интересов сторон.

ФЗ - Федеральный закон.

ФСБ - Федеральная служба безопасности.

ФНС - Федеральная налоговая служба.

ФСТЭК - Федеральная служба по техническому и экспортному контролю.

ИСПДн - Информационная система персональных данных.

3. Основные права и обязанности Оператора и Субъекта персональных данных

3.1. Основные права и обязанности Оператора.

3.1.1. Оператор имеет право:

- самостоятельно определять состав и перечень мер, необходимых и достаточных для обеспечения выполнения обязанностей, предусмотренных Законом № 152-ФЗ и принятыми в соответствии с ним нормативными правовыми актами;

- поручить 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, соблюдать конфиденциальность персональных данных, принимать необходимые меры, направленные на обеспечение выполнения обязанностей, предусмотренных Законом № 152-ФЗ;

- в случае отзыва Субъектом персональных данных согласия на обработку персональных данных Оператор вправе продолжить обработку персональных данных без согласия субъекта персональных данных при наличии оснований, указанных в Законе № 152-ФЗ.

3.1.2. Оператор обязан:

- организовывать обработку персональных данных в соответствии с Законом № 152-ФЗ;

- опубликовать или иным образом обеспечить неограниченный доступ к *настоящей Политике*, к сведениям о реализуемых требованиях к защите персональных данных;

- осуществлять хранение персональных данных в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен федеральным законом, договором;

- отвечать на обращения и запросы Субъектов персональных данных и их законных представителей;

- при сборе персональных данных Оператор обязан предоставить субъекту персональных данных по его просьбе информацию, предусмотренную частью 7 статьи 14 Закона № 152-ФЗ;
- 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 пунктах 2, 3, 4, 8 части 1 статьи 6 Законом 152-ФЗ;
- сообщать в уполномоченный орган по защите прав субъектов персональных данных (Федеральную службу по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор)) по запросу этого органа необходимую информацию в течение 10 рабочих дней с даты получения такого запроса. Данный срок может быть продлен, но не более чем на пять рабочих дней. Для этого Оператору необходимо направить в Роскомнадзор мотивированное уведомление с указанием причин продления срока предоставления запрашиваемой информации;
- в порядке, определенном федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, обеспечивать взаимодействие с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы РФ, включая информирование его о компьютерных инцидентах, которые повлекли неправомерную передачу (предоставление, распространение, доступ) персональных данных.

3.2. Основные права Субъекта персональных данных.

Субъект персональных данных имеет право:

- получать информацию, касающуюся обработки его персональных данных, за исключением случаев, предусмотренных федеральными законами. Сведения предоставляются субъекту персональных данных Оператором в доступной форме, и в них не должны содержаться персональные данные, относящиеся к другим субъектам персональных данных, за исключением случаев, когда имеются законные основания для раскрытия таких персональных данных. Перечень информации и порядок ее получения установлен Законом № 152-ФЗ;
- 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 иные предусмотренные законом меры по защите своих прав;
- дать предварительное согласие при обработке персональных данных в целях продвижения на рынке товаров, работ и услуг;
- обжаловать в Роскомнадзоре или в судебном порядке неправомерные действия или бездействие Оператора при обработке его персональных данных.

4. Цели сбора и сроки обработки персональных данных

4.1. Основной целью сбора и обработки ПДн является обработка персональных данных работников Организации и пациентов медицинской организации (законных представителей).

4.2. Обработка персональных данных пациентов осуществляется в медико-профилактических целях, в целях установления медицинского диагноза, оказания платных медицинских (стоматологических) услуг.

4.2.1. Обеспечение организации оказания медицинской помощи населению, а также наиболее полного исполнения обязательств и компетенций в соответствии с требованиями Федерального закона от 21.11.2011г. № 323-ФЗ «Об основах охраны здоровья граждан Российской Федерации», Правилами предоставления медицинскими организациями платных медицинских услуг, утвержденными Постановлением Правительства Российской Федерации № 736 от 11.05.2023 г.

4.3. Обработка персональных данных работников (бывших работников, кандидатов на работу) осуществляется в целях:

4.3.1. Оформления трудовых отношений.

4.3.2. Ведение кадрового и бухгалтерского учета.

4.3.3. Заключение, исполнения и прекращения гражданско-правовых отношений.

4.3.4. Исполнение требований налогового законодательства по вопросам исчисления и уплаты налога на доходы физических лиц, взносов во внебюджетные фонды и страховых взносов во внебюджетные фонды, пенсионного законодательства при формировании и передаче в ПФР персоналифицированных данных о каждом получателе доходов, которые учитываются при начислении взносов на обязательное пенсионное страхование.

4.3.5. Заполнение первичной статистической документации в соответствии с трудовым, налоговым законодательством и иными федеральными законами, а также в иных случаях установленных в законе.

4.4. Обработка персональных данных осуществляется также с целью продвижения товаров, работ, услуг на рынке, путем использования официального сайта Организации в сети Интернет.

4.5. Обработка персональных данных должна осуществляться на законной основе.

4.6. Обработка персональных данных должна ограничиваться достижением конкретных, заранее определенных и законных целей. Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных.

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

4.8. Обработке подлежат только персональные данные, которые отвечают целям их обработки.

4.9. Обработка персональных данных осуществляется Оператором с учетом сроков, указанных в согласии субъекта на обработку его персональных данных (указания конкретной даты, периода, события).

4.10. Оператор прекращает обработку персональных данных в следующих случаях:

- выявлен факт их неправомерной обработки (срок - в течение трех рабочих дней с даты выявления);

- достигнута цель их обработки;

- истек срок действия или отозвано согласие субъекта персональных данных на обработку указанных данных, когда Законом № 152-ФЗ обработка этих данных допускается только с согласия.

4.10.1. При достижении целей обработки персональных данных, а также в случае отзыва субъектом персональных данных согласия на их обработку Оператор прекращает обработку этих данных, если:

- иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных;

- Оператор не вправе осуществлять обработку без согласия субъекта персональных данных на основаниях, предусмотренных Законом № 152-ФЗ или иными федеральными законами;

- иное не предусмотрено другим соглашением между Оператором и субъектом персональных данных.

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

5.1. Содержание и объем обрабатываемых персональных данных должны соответствовать заявленным целям обработки, предусмотренным в разделе 4 настоящей Политики.

Обрабатываемые персональные данные не должны быть избыточными по отношению к заявленным целям их обработки.

5.2. Оператор может обрабатывать персональные данные следующих категорий субъектов персональных данных:

- физические лица (работники), состоящие с Организацией в трудовых отношениях;

- физические лица, уволившиеся из Организации (бывшие работники);

- физические лица, являющиеся близкими родственниками работников Организации;

- физические лица, являющиеся кандидатами на работу;

- физические лица, обратившиеся в Организацию за медицинской помощью и их законные представители;

- физические лица, состоящие в гражданско-правовых отношениях (контрагенты) с Организацией;

- физические лица, пользователи сайта Организации.

5.3. В целях соблюдения требований действующего законодательства Оператор осуществляет обработку ПДн субъектов персональных данных, указанных в пункте 5.2. содержащие нижеприведенные критерии, сведения и информацию.

5.3.1. Работники и бывшие работники Оператора:

- фамилия, имя, отчество (последнее при наличии) (в том числе прежние фамилии, имена или отчества, в случае их изменения);

- пол;

- гражданство;

- дата и место рождения;

- паспортные данные;

- вид, серия, номер документа, удостоверяющего личность гражданина Российской Федерации, наименование органа, код подразделения выдавшего его, дата выдачи;

- адрес регистрации по месту жительства;

- адрес фактического проживания;
- контактные данные (номер телефона, адрес электронной почты, сведения об иных средствах связи);
- индивидуальный номер налогоплательщика (ИНН);
- страховой номер индивидуального лицевого счета (СНИЛС);
- сведения об образовании, квалификации, профессиональной подготовке и повышении квалификации;
- семейное положение, наличие детей, родственные связи;
- сведения о трудовой деятельности, в том числе об отпусках; наличии поощрений, наградений и (или) дисциплинарных взысканий;
- данные о регистрации брака;
- сведения о воинском учете;
- сведения об инвалидности;
- сведения об удержании алиментов;
- сведения о доходе с предыдущего места работы;
- изображение (фотография);
- специальные персональные данные: сведения о наличии или отсутствии судимости; сведения о состоянии здоровья, влияющие на выполнение трудовой функции.

5.3.1.1. В целях ведения персонифицированного учета осуществляется обработка следующих персональных данных *о лицах, которые участвуют в осуществлении медицинской деятельности* в соответствии с требованиями статьи 93 Закона 323-ФЗ:

- фамилия, имя, отчество (последнее при наличии);
- пол;
- дата рождения; место рождения;
- гражданство;
- данные документа, удостоверяющего личность;
- место жительства;
- место регистрации;
- дата регистрации;
- страховой номер индивидуального лицевого счета;
- контактные данные (номер телефона, адрес электронной почты);
- сведения об образовании, об обучении или о периоде обучения, в том числе данные об организациях, осуществляющих образовательную деятельность по реализации профессиональных образовательных программ медицинского образования и фармацевтического образования, о документах об образовании и (или) о квалификации, о договоре о целевом обучении, а также данные о сертификате специалиста или о прохождении аккредитации специалиста, сведения о результатах сдачи экзамена для получения допуска к осуществлению медицинской деятельности;
- наименование организации, осуществляющей медицинскую деятельность;
- занимаемая должность в организации, осуществляющей медицинскую деятельность.

5.3.2. *Члены семьи работников Оператора:*

- фамилия, имя, отчество (последнее при наличии);
- степень родства;
- год рождения.

5.3.3. *Кандидаты для приема на работу к Оператору:*

- фамилия, имя, отчество (последнее при наличии);
- пол;
- гражданство;
- дата и место рождения;
- контактные данные (номер телефона, адрес электронной почты);
- сведения об образовании, опыте работы, квалификации;
- иные персональные данные, сообщаемые кандидатами в резюме и сопроводительных письмах.

5.3.4. *Клиенты Оператора физические лица:*

5.3.4.1. *Пациенты*, с учетом требований статьи 94 Закона 323-ФЗ в системе персонифицированного учета Организации осуществляется обработка следующих персональных данных о лицах, которым оказывается медицинская помощь:

- фамилия, имя, отчество (последнее при наличии);

- пол;
- дата рождения;
- место рождения;
- гражданство;
- данные документа, удостоверяющего личность (паспортные данные; свидетельство о рождении);
 - место жительства;
 - место регистрации;
 - дата регистрации;
 - страховой номер, индивидуального лицевого счета;
 - номер полиса обязательного медицинского страхования застрахованного лица (при наличии);
 - анамнез;
 - диагноз;
 - сведения об организации, осуществляющей медицинскую деятельность;
 - вид оказанной медицинской помощи;
 - условия оказания медицинской помощи;
 - сроки оказания медицинской помощи;
 - объем оказанной медицинской помощи, включая сведения об оказанных медицинских услугах;
 - результат обращения за медицинской помощью;
 - серия и номер выданного листка нетрудоспособности (при наличии);
 - сведения о проведенных медицинских экспертизах, медицинских осмотрах и медицинских освидетельствованиях и их результаты;
 - примененные клинические рекомендации;
 - сведения о медицинском работнике или медицинских работниках, оказавших медицинскую помощь, проводивших медицинские экспертизы, медицинские осмотры и медицинские освидетельствования;
 - данные, способствующие идентификации личности: слепки, рентгеновские снимки, фотографии, видеоизображения с установленных систем видеонаблюдения;
 - другие сведения, характеризующие физиологические и биологические особенности пациента, на основании которых можно установить личность;
- контактные данные (номер телефона, адрес электронной почты);
- сведения о законном представителе (при наличии).

5.3.4.2. **Законные представители пациентов:**

- фамилия, имя, отчество (последнее при наличии);
- дата рождения;
- паспортные данные;
- адрес регистрации;
- контактные данные (номер телефона, адрес электронной почты).

5.3.5. **Контрагенты Оператора (физические лица):**

- фамилия, имя, отчество (последнее при наличии);
- дата и место рождения;
- паспортные данные;
- адрес регистрации,
- адрес места жительства;
- контактные данные (номер телефона, адрес электронной почты);
- замещаемая должность;
- индивидуальный номер налогоплательщика;
- номер расчетного счета.

5.3.6. **Представители (работников, клиентов и контрагентов Оператора (юридических лиц):**

- фамилия, имя, отчество (последнее при наличии);
- паспортные данные;
- контактные данные (номер телефона, адрес электронной почты);
- замещаемая должность.

5.3.7. **Пользователи сайта Организации:**

- фамилия, имя, отчество (последнее при наличии);
- контактные данные (номер телефона, адрес электронной почты);

- сведения, собираемые посредством метрических программ.

5.4. Обработка Оператором биометрических персональных данных (сведений, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность) осуществляется в соответствии с законодательством Российской Федерации.

5.5. Оператором не осуществляется обработка специальных категорий персональных данных, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, интимной жизни, за исключением случаев, предусмотренных законодательством РФ.

6. Принципы обеспечения безопасности персональных данных

6.1. Основной задачей обеспечения безопасности ПДн при их обработке в Организации является предотвращение несанкционированного доступа к ним третьих лиц, предупреждение преднамеренных программно-технических и иных воздействий с целью хищения ПДн, разрушения (уничтожения) или искажения их в процессе обработки.

6.2. Для обеспечения безопасности ПДн Организация руководствуется следующими принципами:

- законность: защита ПДн основывается на положениях нормативных правовых актов и методических документов уполномоченных государственных органов в области обработки и защиты ПДн;

- системность: обработка ПДн в Организации осуществляется с учетом всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, значимых для понимания и решения проблемы обеспечения безопасности ПДн;

- комплексность: защита ПДн строится с использованием функциональных возможностей информационных технологий, реализованных в информационных системах Организации и других имеющихся в Организации систем и средств защиты;

- непрерывность: защита ПДн обеспечивается на всех этапах их обработки и во всех режимах функционирования систем обработки ПДн, в том числе при проведении ремонтных и регламентных работ;

- своевременность: меры, обеспечивающие надлежащий уровень безопасности ПДн, принимаются до начала их обработки;

- преемственность и непрерывность совершенствования: модернизация и наращивание мер и средств защиты ПДн осуществляется на основании результатов анализа практики обработки ПДн в Организации с учетом выявления новых способов и средств реализации угроз безопасности ПДн, отечественного и зарубежного опыта в сфере защиты информации;

- персональная ответственность: ответственность за обеспечение безопасности ПДн возлагается на работников в пределах их обязанностей, связанных с обработкой и защитой ПДн;

- минимизация прав доступа: доступ к ПДн предоставляется работникам только в объеме, необходимом для выполнения их должностных обязанностей;

- гибкость: обеспечение выполнения функций защиты ПДн при изменении характеристик функционирования информационных систем персональных данных Организации, а также объема и состава обрабатываемых ПДн;

- специализация и профессионализм: реализация мер по обеспечению безопасности ПДн осуществляются Работниками, имеющими необходимые для этого квалификацию и опыт;

- эффективность процедур отбора кадров: кадровая политика Организации предусматривает тщательный подбор персонала и мотивацию работников, позволяющую исключить или минимизировать возможность нарушения ими безопасности ПДн;

- наблюдаемость и прозрачность: меры по обеспечению безопасности ПДн должны быть спланированы так, чтобы результаты их применения были явно наблюдаемы (прозрачны) и могли быть оценены лицами, осуществляющими контроль;

- непрерывность контроля и оценки: устанавливаются процедуры постоянного контроля использования систем обработки и защиты ПДн, а результаты контроля регулярно анализируются.

6.3. В Организации не производится обработка ПДн, несовместимая с целями их сбора.

Если иное не предусмотрено федеральным законом, по окончании обработки ПДн в Организации, в том числе при достижении целей их обработки или утраты необходимости в достижении этих целей, обрабатывавшиеся Организацией ПДн уничтожаются или обезличиваются.

6.4. При обработке ПДн обеспечиваются их точность, достаточность, а при необходимости – и актуальность по отношению к целям обработки. Организация принимает необходимые меры по удалению или уточнению неполных или неточных ПДн.

7. Порядок, условия обработки и сроки хранения персональных данных

7.1. Обработка персональных данных осуществляется Оператором в соответствии с требованиями законодательства Российской Федерации.

7.2. Обработка персональных данных осуществляется с согласия субъектов персональных данных на обработку их персональных данных, а также без такового в случаях, предусмотренных законодательством Российской Федерации.

7.3. Оператор осуществляет как автоматизированную, так и неавтоматизированную обработку персональных данных, а также смешанную обработку персональных данных.

7.4. К обработке персональных данных допускаются работники Оператора, в должностные обязанности которых входит обработка персональных данных.

7.5. Обработка персональных данных осуществляется путем:

- получения персональных данных в устной и письменной форме непосредственно от субъектов персональных данных;

- получения персональных данных из общедоступных источников;

- внесения персональных данных в журналы, реестры и информационные системы Оператора;

- использования иных способов обработки персональных данных.

7.6. Не допускается раскрытие третьим лицам и распространение персональных данных без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.

Согласие на обработку персональных данных, разрешенных субъектом персональных данных для распространения, оформляется отдельно от иных согласий субъекта персональных данных на обработку его персональных данных. Требования к содержанию согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения, утверждены Приказом Роскомнадзора от 24.02.2021 г. № 18.

7.7. Передача персональных данных органам дознания и следствия, в Федеральную налоговую службу, Пенсионный фонд Российской Федерации, Фонд социального страхования и другие уполномоченные органы исполнительной власти и организации осуществляется в соответствии с требованиями законодательства Российской Федерации.

7.8. Оператор принимает необходимые правовые, организационные и технические меры для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, распространения и других несанкционированных действий, в том числе:

- определяет угрозы безопасности персональных данных при их обработке;

- издает настоящую Политику,

- издает Политику конфиденциальности интернет сайта организации;

- утверждает отдельные положения по обработке и защите персональных данных работников клиентов (пациентов) Оператора;

- принимает иные локальные нормативные акты и иные документы, регулирующие отношения в сфере обработки и защиты персональных данных;

- назначает лиц, ответственных за обеспечение безопасности персональных данных в структурных подразделениях и информационных системах Оператора;

- создает необходимые условия для работы с персональными данными;

- организует учет документов, содержащих персональные данные;

- организует работу с информационными системами, в которых обрабатываются персональные данные;

- хранит персональные данные в условиях, при которых обеспечивается их сохранность и исключается неправомерный доступ к ним;

- знакомит работников с настоящей Политикой, внутренними локальными и распорядительными актами, принимаемыми в целях соблюдения требований по охране и защите персональных данных;

- на постоянной основе организует обучение работников Оператора, осуществляющих обработку персональных данных.

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

7.9.1. **Персональные данные зафиксированные на бумажных носителях, хранятся в специально отведенных для этого местах в сейфах, специальных запираемых шкафах, расположенных в запираемых помещениях с ограниченным правом доступа.**

7.9.2. Персональные данные субъектов, обрабатываемые с использованием средств автоматизации в разных целях, хранятся в специальных папках (вкладках).

7.9.3. Не допускается хранение и размещение документов, содержащих ПДн, в открытых электронных каталогах.

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

7.11. Хранение персональных данных на бумажных носителях осуществляется Оператором с учетом сроков хранения документов, для которых эти сроки предусмотрены законодательством об архивном деле в РФ (Федеральный закон от 22.10.2004 г. № 125-ФЗ «Об архивном деле в Российской Федерации»). Перечень типовых управленческих архивных документов, образующихся в процессе деятельности государственных органов, органов местного самоуправления и организаций, с указанием сроков их хранения (утв. Приказом Росархива от 20.12.2019 г. № 236)).

7.11.1. Персональные данные работников хранятся в течение пятидесяти лет после увольнения.

7.11.2. Срок хранения персональных данных клиентов (пациентов) соответствует сроку хранения медицинской карты пациента и составляет двадцать пять лет с последнего приема.

7.12. Срок хранения персональных данных, обрабатываемых в информационных системах персональных данных, соответствует сроку хранения персональных данных на бумажных носителях.

7.13. Персональные данные субъектов, обрабатываемые Организацией, подлежат уничтожению либо обезличиванию в случае:

- достижения целей обработки ПДн или утраты необходимости в достижении этих целей;
- отзыва субъектом ПДн согласия на обработку его ПДн;
- истечение срока действия согласия субъекта ПДн на обработку его ПДн;
- отсутствия возможности обеспечить правомерность обработки ПДн;
- прекращения деятельности Организации.

7.14. Порядок уничтожения персональных данных Оператором.

7.14.1. Условия и сроки уничтожения персональных данных Оператором:

• достижение цели обработки персональных данных либо утрата необходимости достигать эту цель - **в течение 30 дней**;

• достижение максимальных сроков хранения документов, содержащих персональные данные, - **в течение 30 дней**;

• предоставление субъектом персональных данных (его представителем) подтверждения того, что персональные данные получены незаконно или не являются необходимыми для заявленной цели обработки, - **в течение семи рабочих дней**;

• отзыв субъектом персональных данных согласия на обработку его персональных данных, если их сохранение для цели их обработки более не требуется, - в течение 30 дней.

7.14.3. Уничтожение персональных данных осуществляет комиссия, созданная приказом генерального директора ООО «А-СТОМ». Факт уничтожения ПДн подтверждается документально актом об уничтожении носителей, подписанным членами комиссии.

7.14.4. Способы уничтожения персональных данных устанавливаются в локальных нормативно-правовых актах Оператора.

8. Порядок обработки персональных данных в информационных системах

8.1. При сборе персональных данных, в том числе посредством информационно-телекоммуникационной сети Интернет, запись, систематизация, накопление, хранение, уточнение (обновление, изменение), извлечение персональных данных граждан Российской Федерации с использованием баз данных, находящихся за пределами Российской Федерации, не допускаются, за исключением случаев, указанных в Законе № 152-ФЗ.

8.2. Обработка персональных данных в информационных системах Организации осуществляется после реализации организационных и технических мер по обеспечению безопасности персональных данных, определенных с учетом актуальных угроз безопасности персональных данных и информационных технологий, используемых в информационных системах.

8.3. Уполномоченному работнику, имеющему право осуществлять обработку персональных данных в информационных системах, предоставляется уникальный логин и пароль для доступа к соответствующей информационной системе. Доступ предоставляется в соответствии с функциями, предусмотренными должностными обязанностями работника.

8.4. Информация может вноситься как в автоматическом режиме при получении персональных данных с официального сайта в сети интернет, так и в ручном режиме при получении информации на бумажном носителе или в ином виде, не позволяющем осуществлять ее автоматическую регистрацию.

8.5. Обеспечение безопасности персональных данных, обрабатываемых Оператором в информационных системах, достигается путем исключения несанкционированного, в том числе случайного, доступа к персональным данным.

8.6. В случае выявления нарушений порядка обработки персональных данных уполномоченными

работниками незамедлительно принимаются меры по установлению причин нарушений и их устранению.

8.7. В состав мер по обеспечению безопасности персональных данных, реализуемых Организацией 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;
- управление доступом субъектов доступа к объектам доступа;
- ограничение программной среды;
- защита машинных носителей информации, на которых хранятся и (или) обрабатываются персональные данные;
- регистрация событий безопасности;
- антивирусная защита;
- обнаружение (предотвращение) вторжений;
- контроль (анализ) защищенности персональных данных;
- обеспечение целостности информационной системы и персональных данных;
- обеспечение доступности персональных данных;
- защита среды виртуализации и технических средств;
- защита информационной системы, ее средств, систем связи и передачи 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 и системы защиты персональных данных.

8.8. Под актуальными угрозами безопасности персональных данных в Организации 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.

Угрозы первого типа актуальны для информационной системы, если для нее, в том числе актуальны угрозы, связанные с наличием недокументированных (недекларированных) возможностей в системном программном обеспечении, используемом в информационной системе.

Угрозы второго типа актуальны для информационной системы, если для нее в том числе актуальны угрозы, связанные с наличием недокументированных (недекларированных) возможностей в прикладном программном обеспечении, используемом в информационной системе.

Угрозы третьего типа актуальны для информационной системы, если для нее актуальны угрозы, не связанные с наличием недокументированных (недекларированных) возможностей в системном и прикладном программном обеспечении, используемом в информационной системе.

8.8.1. Определение типа угроз безопасности персональных данных, актуальных для информационной системы, производится в Организации с учетом оценки возможного вреда, проведенной во исполнение пункта 5 части 1 статьи 18.1 Закона о персональных данных».

8.8.2. Оценка вреда, который может быть причинен субъектам персональных данных ООО «А-СТОМ» проводится Оператором согласно правил оценки вреда, разработанных в соответствии с Приказом Роскомнадзора от 27.10.2022 г. № 178 «Об утверждении Требований к оценке вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона «О персональных данных».

8.9. В соответствии с пунктом 11 статьи 19 Закона № 152-ФЗ под уровнем защищенности персональных данных понимается комплексный показатель, характеризующий требования, исполнение которых обеспечивает нейтрализацию определенных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Уровень защищенности при обработке персональных данных в информационных системах определяется отдельным локальным (распорядительным) актом.

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

9.1. Подтверждение факта обработки персональных данных Оператором, правовые основания и цели обработки персональных данных, а также иные сведения, указанные в части 7 статьи 14 Закона № 152-ФЗ, предоставляются Оператором субъекту персональных данных или его представителю **в течение 10 рабочих дней с момента обращения либо получения запроса субъекта персональных данных**

или его представителя. Данный срок может быть продлен, но не более чем на пять рабочих дней. Для этого Оператору следует направить субъекту персональных данных мотивированное уведомление с указанием причин продления срока предоставления запрашиваемой информации.

В предоставляемые сведения не включаются персональные данные, относящиеся к другим субъектам персональных данных, за исключением случаев, когда имеются законные основания для раскрытия таких персональных данных.

Запрос должен содержать:

- номер основного документа, удостоверяющего личность субъекта персональных данных или его представителя, сведения о дате выдачи указанного документа и выдавшем его органе;
- адрес, по которому следует направить ответ, контактный телефон;
- сведения, подтверждающие участие субъекта персональных данных в отношениях с Оператором (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки персональных данных Оператором;
- подпись субъекта персональных данных или его представителя.

Запрос направляется посредством почтовой связи либо предоставляется заявителем лично по месту нахождения Оператора по адресу: Амурская область. г.Благовещенск, ул. Амурская, 208, офис 83.

Запрос может быть направлен в форме электронного документа и подписан электронной подписью в соответствии с законодательством Российской Федерации.

Оператор предоставляет сведения, указанные в части 7 статьи 14 Закона № 152-ФЗ, субъекту персональных данных или его представителю в той форме, в которой направлены соответствующие обращение либо запрос, если иное не указано в обращении или запросе.

Если в обращении (запросе) субъекта персональных данных не отражены в соответствии с требованиями Закона о персональных данных все необходимые сведения или субъект не обладает правами доступа к запрашиваемой информации, то ему направляется мотивированный отказ.

Право субъекта персональных данных на доступ к его персональным данным может быть ограничено в соответствии с части 8 статьи 14 Закона № 152-ФЗ, в том числе если доступ субъекта персональных данных к его персональным данным нарушает права и законные интересы третьих лиц.

9.2. В случае выявления неточных персональных данных при обращении субъекта персональных данных или его представителя либо по их запросу или по запросу Роскомнадзора Оператор осуществляет блокирование персональных данных, относящихся к этому субъекту персональных данных, 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.

В случае подтверждения факта неточности персональных данных Оператор на основании сведений, представленных субъектом персональных данных или его представителем либо Роскомнадзором, или иных необходимых документов уточняет персональные данные в течение семи рабочих дней со дня представления таких сведений и снимает блокирование персональных данных.

9.3. В случае выявления неправомерной обработки персональных данных при обращении (запросе) субъекта персональных данных или его представителя либо Роскомнадзора Оператор осуществляет блокирование неправомерно обрабатываемых персональных данных, относящихся к этому субъекту персональных данных, с момента такого обращения или получения запроса.

9.4. При выявлении Оператором, Роскомнадзором или иным заинтересованным лицом факта неправомерной или случайной передачи (предоставления, распространения) персональных данных (доступа к персональным данным), повлекшей нарушение прав субъектов персональных данных, Оператор:

- **в течение 24 часов** - уведомляет Роскомнадзор о произошедшем инциденте, предполагаемых причинах, повлекших нарушение прав субъектов персональных данных, предполагаемом вреде, нанесенном правам субъектов персональных данных, и принятых мерах по устранению последствий инцидента, а также предоставляет сведения о лице, уполномоченном Оператором на взаимодействие с Роскомнадзором по вопросам, связанным с инцидентом;
- **в течение 72 часов** - уведомляет Роскомнадзор о результатах внутреннего расследования выявленного инцидента и предоставляет сведения о лицах, действия которых стали его причиной (при наличии).

10. Защита персональных данных

10.1. Организация, при обработке ПДн, принимает необходимые правовые, организационные и технические меры, и обеспечивает их принятие для защиты ПДн от неправомерного или случайного

доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения ПДн, а также от иных неправомерных действий в отношении ПДн.

10.2. Основными мерами защиты ПДн, используемыми Организацией, являются:

- определения ответственных лиц за обработку персональных данных;
- назначение лица ответственного за обработку ПДн, которое осуществляет организацию обработки ПДн, обучение и инструктаж, контроль за соблюдением Организацией и его работниками требований к защите ПДн;
- ознакомление работников, осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, Политикой Организации в отношении обработки персональных данных, локальными актами по вопросам обработки персональных данных, и обучение указанных сотрудников;
- издание Политики Организации в отношении обработки персональных данных, внутренних нормативно - правовых (локальных) актов и распорядительных документов по вопросам обработки персональных данных;
- счѐт машинных носителей персональных данных, проведение своевременной инвентаризации;
- определение актуальных угроз безопасности ПДн при их обработке в СЗПД, и разработка мер и мероприятий по защите ПДн;
- актуализация внутренних нормативных (локальных) актов, внесение изменений в настоящую Политику в отношении обработки персональных данных;
- сертифицированное антивирусное программное обеспечение с регулярно обновляемыми базами;
- сертифицированное программное средство защиты информации от несанкционированного доступа:
- соблюдение условий, обеспечивающих сохранность ПДн и исключаящие несанкционированный к ним доступ, оценка эффективности принимаемых и реализованных мер по обеспечению безопасности ПДн;
- обучение работников Организации непосредственно осуществляющих обработку персональных данных, положениям законодательства Российской Федерации о персональных данных, в том числе требованиям к защите персональных данных, документами, определяющими политику Организации в отношении обработки персональных данных, локальным актам по вопросам обработки персональных данных;
- осуществление внутреннего контроля и аудита;
- оценкой эффективности принимаемых мер по обеспечению безопасности персональных данных;
- оценкой вреда, который может быть причинен субъектам персональных данных в случае нарушения законодательства о персональных данных, соотношением указанного вреда и принимаемых оператором мер, направленных на обеспечение обязанностей, предусмотренных законодательством о персональных данных;
- иными мерами, предусмотренными действующим законодательством.

11. Ответственность

11.1. Ответственность за нарушение требований законодательства Российской Федерации и нормативных актов в сфере обработки и защиты персональных данных определяется в соответствии с действующим законодательством Российской Федерации.

11.2. В соответствии с требованиями статьи 24 Закона № 152-ФЗ Оператор несет ответственность за нарушение требований действующего законодательства, регулирующего сферу обработки и защиты персональных данных, которая выражается в виде уголовной, административной, дисциплинарной и иной предусмотренной законодательством Российской Федерации ответственности.

11.3. Оператор несет ответственность за использование персональных данных в целях причинения имущественного и морального вреда субъектам персональных данных, затруднения реализации их прав и свобод. Ограничение прав субъектов персональных данных на основе использования информации об их социальном происхождении, о расовой, национальной принадлежности запрещено.

11.4. В случае нарушения порядка обеспечения безопасности персональных данных, работники Оператора несут гражданскую, административную, уголовную, дисциплинарную ответственность, предусмотренную действующим законодательством Российской Федерации.

12. Заключительные положения

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

12.2. Требования Политики обязательны для выполнения и соблюдения работниками Оператора, которые допущены к работе с персональными данными.

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

12.4. Лицом ответственным за исполнение требований действующего законодательства в сфере обработки и защиты персональных данных является руководитель Организации.

12.5. Контроль за исполнением требований настоящей Политики осуществляется также уполномоченным лицом, ответственным за организацию обработки персональных данных у Оператора и членами комиссии по проведению внутреннего контроля за обработкой персональных данных в Организации.