

СВЕДЕНИЯ

о реализуемых требованиях к защите персональных данных

ООО «Глазная клиника Юго-Запад»

1. Общие положения

1.1. Настоящие Сведения о реализуемых требованиях к защите персональных данных (далее — Сведения) разработаны в соответствии со статьёй 18.1 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» (далее — Закон о персональных данных), Постановлением Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», Постановлением Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», а также иными нормативными правовыми актами Российской Федерации в области защиты персональных данных.

1.2. Сведения определяют требования к обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных и без использования средств автоматизации, эксплуатируемых ООО «Глазная клиника Юго-Запад» (далее — Оператор).

1.3. Сведения подлежат размещению на официальном сайте Оператора в информационно-телекоммуникационной сети «Интернет» по адресу: <https://gadzhiev-clinic.ru>.

2. Сведения об Операторе

2.1. Полное наименование: Общество с ограниченной ответственностью «Глазная клиника Юго-Запад».

2.2. Адрес местонахождения: 355014, Ставропольский край, г. Ставрополь, ул. Доваторцев, д. 86/1, 86/2.

2.3. Контактный телефон: +7 (8652) 91-94-49.

2.4. Адрес электронной почты: glazklinik@gmail.com.

2.5. Сайт в сети «Интернет»: <https://gadzhiev-clinic.ru>.

3. Категории обрабатываемых персональных данных

3.1. Оператор обрабатывает следующие категории персональных данных субъектов:

— фамилия, имя, отчество;

- дата рождения;
- адрес регистрации и фактического проживания;
- номер контактного телефона;
- адрес электронной почты;
- паспортные данные (серия, номер, дата выдачи, кем выдан, код подразделения);
- сведения о полисе ОМС / ДМС (номер, наименование страховой организации);
- сведения о состоянии здоровья (диагнозы, результаты обследований, медицинская карта пациента) — специальные категории персональных данных в соответствии со статьёй 10 Закона о персональных данных;
- сведения о трудовой деятельности (в отношении работников Оператора).

3.2. К субъектам персональных данных относятся:

- пациенты Оператора (действующие и потенциальные);
- законные представители пациентов;
- работники Оператора;
- посетители сайта <https://gadzhiev-clinic.ru>;
- контрагенты и представители контрагентов Оператора.

4. Правовые основания обработки персональных данных

4.1. Обработка персональных данных осуществляется на следующих правовых основаниях:

- согласие субъекта персональных данных на обработку его персональных данных;
- заключение и исполнение договора, стороной которого является субъект персональных данных;
- требования федерального закона от 21.11.2011 № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации» в части ведения медицинской документации;
- требования Трудового кодекса Российской Федерации в части обработки персональных данных работников;
- осуществление прав и законных интересов Оператора и третьих лиц при условии, что при этом не нарушаются права и свободы субъекта персональных данных.

5. Цели обработки персональных данных

5.1. Персональные данные обрабатываются в следующих целях:

- оказание медицинских услуг пациентам, ведение медицинской документации;
- запись пациентов на приём, организация лечебного процесса;
- заключение и исполнение договоров на оказание медицинских услуг;
- информирование пациентов о результатах обследований, назначениях и рекомендациях;
- обратная связь, в том числе направление уведомлений, напоминаний о визитах;
- обеспечение внутреннего контроля качества оказания медицинских услуг;
- кадровое обеспечение, оформление трудовых отношений с работниками;
- ведение бухгалтерского и налогового учёта.

6. Актуальные угрозы безопасности персональных данных

6.1. При обработке персональных данных в информационных системах персональных данных (далее — ИСПДн) Оператор учитывает следующие актуальные угрозы:

- несанкционированный доступ к персональным данным с использованием штатных и нештатных (вредоносных) программных средств;
- несанкционированное копирование персональных данных с машинных носителей информации;
- утечка информации по техническим каналам (электромагнитные излучения, наводки на технические линии);
- утрата (разрушение, искажение) персональных данных в результате сбоев оборудования, ошибок пользователей, программных сбоев;
- несанкционированный доступ к персональным данным лиц, не имеющих права доступа;
- модификация, уничтожение и (или) блокирование персональных данных в результате воздействия вредоносного программного обеспечения.

6.2. Для выявления и оценки актуальных угроз Оператор проводит оценку уровня защищённости ИСПДн в соответствии с требованиями нормативных правовых актов Российской Федерации.

7. Уровень защищённости персональных данных

7.1. В соответствии с постановлением Правительства Российской Федерации от 01.11.2012 № 1119 Оператор определяет уровень защищённости персональных данных для каждой ИСПДн. Обработка специальных категорий персональных данных (сведения о состоянии здоровья) в ИСПДн, имеющей подключение к сети «Интернет» и (или) к иным сетям электросвязи,

соответствует уровню защищённости «1» (высокий). Обработка иных категорий персональных данных соответствует уровню защищённости не ниже «3» (низкий) или «2» (средний) в зависимости от типа ИСПДн и количества субъектов.

8. Реализуемые требования к защите персональных данных

8.1. Организационные меры защиты:

- назначение лица, ответственного за организацию обработки персональных данных;
- издание локальных нормативных актов Оператора, регулирующих порядок обработки и обеспечения безопасности персональных данных;
- ограничение круга сотрудников, имеющих доступ к персональным данным, на основе принципа минимально необходимых полномочий;
- ознакомление работников под роспись с локальными нормативными актами по защите персональных данных;
- проведение обучения работников, осуществляющих обработку персональных данных, по вопросам их защиты;
- осуществление учёта и хранения машинных носителей персональных данных в установленном порядке;
- контроль соблюдения требований к защите персональных данных со стороны ответственного лица;
- фиксация фактов несанкционированного доступа к персональным данным и реагирование на такие факты.

8.2. Технические (программно-аппаратные) меры защиты:

- применение средств защиты информации (далее — СЗИ), прошедших установленный порядок оценки соответствия;
- обеспечение антивирусной защиты рабочих станций и серверов с использованием сертифицированных или рекомендуемых ФСТЭК России средств антивирусной защиты;
- использование межсетевых экранов для защиты ИСПДн от несанкционированного доступа из внешних сетей;
- обеспечение идентификации и аутентификации пользователей ИСПДн (использование учётных записей и паролей, сложных паролей);
- разграничение прав доступа пользователей ИСПДн в соответствии с должностными обязанностями;

- регистрация и учёт действий пользователей ИСПДн (ведение журналов аудита);
- обеспечение целостности персональных данных и контроль несанкционированных изменений;
- использование средств резервного копирования персональных данных;
- защита машинных носителей персональных данных от несанкционированного доступа;
- обеспечение защиты информационной системы от вредоносного программного обеспечения;
- контроль защищённости персональных данных с использованием средств анализа защищённости.

8.3. Правовые меры защиты:

- обеспечение заключения соглашений о конфиденциальности с работниками, имеющими доступ к персональным данным;
- включение в трудовые договоры с работниками положений о неразглашении персональных данных;
- обеспечение соблюдения условий конфиденциальности при передаче персональных данных третьим лицам по договору.

8.4. Физические меры защиты:

- ограничение физического доступа к помещениям, в которых расположены технические средства ИСПДн;
- размещение серверного оборудования в помещениях с ограниченным доступом;
- обеспечение сохранности носителей персональных данных (бумажных и электронных).

9. Порядок обработки персональных данных без использования средств автоматизации

9.1. Обработка персональных данных без использования средств автоматизации (на бумажных носителях) осуществляется с соблюдением следующих требований:

- хранение бумажных носителей в условиях, исключающих их хищение, потерю, искажение и несанкционированный доступ;
- ведение учёта поступления, движения и уничтожения бумажных носителей персональных данных;
- ограничение доступа лиц к бумажным носителям персональных данных на основе принципа необходимости;
- обеспечение уничтожения бумажных носителей персональных данных по достижении целей обработки или утрате необходимости в их достижении.



10. Трансграничная передача персональных данных

10.1. Оператор не осуществляет трансграничную передачу персональных данных.

11. Ответственность

11.1. Лица, виновные в нарушении норм, регулирующих обработку и защиту персональных данных, несут ответственность в соответствии с действующим законодательством Российской Федерации (гражданско-правовая, административная, уголовная).

12. Заключительные положения

12.1. Настоящие Сведения подлежат пересмотру в случае изменения законодательства Российской Федерации в области защиты персональных данных, а также при изменении процессов обработки персональных данных Оператором.

12.2. Сведения вступают в силу с момента их размещения на сайте Оператора по адресу <https://gadzhiev-clinic.ru> и действуют до их замены новой редакцией.

ООО «Глазная клиника Юго-Запад»

Адрес: 355014, г. Ставрополь, ул. Доваторцев, 86/1, 86/2

Телефон: +7 (8652) 91-94-49

E-mail: glazklinik@gmail.com

Сайт: <https://gadzhiev-clinic.ru>