ПОЛИТИКА КОНФИДЕНЦИАЛЬНОСТИ

в отношении обработки персональных данных

Оператор персональных данных: Мамутова Диляра Сеитосмановна

ИНН: 910906951775, ОГРН:

Руководитель: Мамутова Диляра Сеитосмановна (Самозанятый)

E-mail для обращений по вопросам ПДн: mds250480@mail.ru

Веб-сайт: dusha.source-ltd.com

1. Общие положения

1.1. Настоящая Политика конфиденциальности (далее — Политика) определяет порядок обработки и защиты персональных данных физических лиц (далее — Субъекты), которые пользуются сервисом онлайн-записи, чат-виджетом и иными функциями, размещёнными на сайте dusha.source-ltd.com (далее — Сайт).

1.2. Политика разработана в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» (далее — 152-ФЗ), Постановлением Правительства РФ от 01.11.2012 № 1119, Приказом ФСТЭК России от 18.02.2013 № 21 и иными нормативными правовыми актами Российской Федерации.

1.3. Используя Сайт и/или передавая свои персональные данные Оператору, Субъект выражает согласие с условиями настоящей Политики. В случае несогласия Субъект должен прекратить использование Сайта.

1.4. Оператор оставляет за собой право вносить изменения в настоящую Политику. Актуальная редакция размещается на Сайте.

2. Цели обработки персональных данных

2.1. Оператор обрабатывает персональные данные в следующих целях:

- оказание услуг онлайн-записи на приём (запись к мастеру / специалисту);
- идентификация Субъекта при обращении за услугой;
- связь с Субъектом для подтверждения, переноса или отмены записи;
- отправка напоминаний о предстоящих визитах (в том числе через мессенджеры);
- ведение истории визитов и предпочтений Субъекта для повышения качества обслуживания;
- обработка обращений и обратной связи;
- направление рекламных и информационных сообщений (при наличии отдельного согласия);

• выполнение требований законодательства Российской Федерации.

3. Состав обрабатываемых персональных данных

3.1. Оператор обрабатывает следующие категории персональных данных:

Категория данных	**Перечень данных**	**Цель / Основание**	**Срок хранения**
Основные	ФИО, номер телефона	Запись на приём, идентификация (ст. 6 ч. 1 п. 5 152-ФЗ)	3 года с последнего визита
Контактные	Адрес электронной почты (при предоставлении)	Уведомления, обратная связь (согласие)	3 года с последнего визита
Идентификаторы в мессенджерах	Telegram Chat ID	Подтверждение записи, напоминания (согласие)	До отзыва согласия
Данные визитов	Дата и время записей, выбранные услуги, комментарии	Исполнение договора оказания услуг	3 года с даты визита
Технические данные	IP-адрес, User-Agent (тип браузера/ устройства)	Безопасность, журналирование согласий (ст. 6 ч. 1 п. 6 152-ФЗ)	5 лет (журнал согласий)
Дополнительные поля	Иные данные, указанные в форме записи (при наличии настроенных полей)	Повышение качества обслуживания (согласие)	3 года с последнего визита

3.2. Оператор не осуществляет обработку специальных категорий персональных данных (расовая принадлежность, состояние здоровья, биометрические данные и др.).

4. Правовые основания обработки

4.1. Обработка персональных данных осуществляется на следующих основаниях:

- согласие Субъекта персональных данных (ст. 6 ч. 1 п. 1 152-ФЗ);
- исполнение договора, стороной которого является Субъект (ст. 6 ч. 1 п. 5 152-ФЗ);
- обеспечение безопасности и предотвращение мошенничества (ст. 6 ч. 1 п. 7 152-ФЗ).

5. Порядок обработки персональных данных

5.1. Обработка включает: сбор, запись, систематизацию, накопление, хранение, уточнение, извлечение, использование, передачу, обезличивание, блокирование, удаление, уничтожение.

5.2. Обработка осуществляется с использованием средств автоматизации и в информационных системах персональных данных.

5.3. Персональные данные хранятся в электронном виде на серверах, расположенных на территории Российской Федерации (Россия, г. Москва).

6. Передача персональных данных третьим лицам

6.1. Оператор вправе привлекать для обработки персональных данных следующих лиц:

- Общество с ограниченной ответственностью «СОУРС» (ИНН: 9200000149) — лицензиар программного обеспечения для онлайн-записи, осуществляющий техническую поддержку на основании лицензионного договора;
- Telegram Messenger Inc. — для отправки уведомлений через Telegram-бота (при наличии согласия Субъекта);
- провайдеры хостинга и дата-центров (на территории РФ).

6.2. Передача данных третьим лицам осуществляется на основании договоров, содержащих условия конфиденциальности и безопасности данных.

6.3. Трансграничная передача персональных данных не осуществляется, за исключением случаев использования мессенджеров (Telegram), о чём Субъект уведомляется при получении согласия.

7. Использование технологий искусственного интеллекта

7.1. Сайт может использовать чат-виджет с элементами искусственного интеллекта (AI-ассистент) для обработки обращений Субъектов.

7.2. При взаимодействии с AI-ассистентом сохраняются: содержание сообщений Субъекта, ответы системы, идентификатор сессии.

7.3. Данные, полученные AI-ассистентом, используются исключительно для целей оказания услуг и не передаются третьим лицам для целей, не связанных с функционированием сервиса. Для защиты данных AI-ассистента применяются следующие меры:

- обезличивание данных сессий при хранении (идентификатор сессии не связан с ФИО напрямую);
- шифрование данных при передаче между клиентом и сервером (TLS 1.2+);
- автоматическое удаление данных сессий по истечении срока хранения;
- ограничение доступа к журналам AI-сессий (только администраторы Оператора).

8. Сроки обработки и хранения

8.1. Персональные данные хранятся не дольше, чем этого требуют цели обработки.

8.2. По общему правилу данные хранятся в течение 3 (трёх) лет с момента последнего взаимодействия с Субъектом, после чего подлежат уничтожению или обезличиванию.

8.3. Детализация сроков хранения по категориям:

- ФИО, телефон, e-mail, данные визитов — 3 года с момента последнего визита или обращения;
- идентификаторы в мессенджерах (Telegram Chat ID) — до момента отзыва согласия Субъектом;
- IP-адрес и данные устройства (User-Agent) — 5 лет с даты фиксации (в составе журнала согласий);
- содержание сообщений AI-ассистента (чат-виджет) — 1 (один) год с даты сессии, после чего данные автоматически удаляются или обезличиваются;
- дополнительные поля (настраиваемые поля формы записи) — 3 года с момента последнего визита;
- журнал согласий (ConsentLog) — 5 (пять) лет с даты получения согласия.

8.4. Указанные сроки могут быть сокращены по запросу Субъекта (ст. 14 152-ФЗ) или продлены в случаях, предусмотренных законодательством.

9. Права Субъекта персональных данных

9.1. Субъект имеет право:

- получить информацию об обработке своих персональных данных (ст. 14 152-ФЗ);
- потребовать уточнения, блокирования или уничтожения своих персональных данных (ст. 14 152-ФЗ);
- отозвать согласие на обработку персональных данных (ст. 9 ч. 2 152-ФЗ);
- обжаловать действия Оператора в Роскомнадзор или в суд (ст. 17 152-ФЗ).

9.2. Для реализации прав Субъект направляет обращение на адрес электронной почты: mds250480@mail.ru.

9.3. Оператор обязуется рассмотреть обращение в течение 10 рабочих дней.

10. Меры по защите персональных данных

10.1. Оператор принимает необходимые правовые, организационные и технические меры для защиты персональных данных от неправомерного доступа, уничтожения, изменения, блокирования, копирования, распространения, а также от иных неправомерных действий.

10.2. Для обеспечения безопасности персональных данных применяется комплекс технических мер, включающий шифрование каналов связи по протоколу TLS 1.2 и выше (предотвращает перехват данных при передаче), межсетевое экранирование (firewall) серверной инфраструктуры, хеширование паролей алгоритмом bcrypt, ролевую модель разграничения доступа, журналирование действий пользователей и администраторов, а также регулярное резервное копирование. Ниже приводится детализация каждой меры:

- шифрование данных при передаче (HTTPS/TLS 1.2+) — все соединения между браузером пользователя и сервером защищены SSL-сертификатом, что исключает перехват данных при передаче;
- ограничение доступа к персональным данным (ролевая модель доступа: admin / owner / master) — каждый пользователь системы видит только те данные, которые необходимы для выполнения его функций;
- хранение паролей в хешированном виде (bcrypt) — даже при несанкционированном доступе к базе данных восстановление паролей невозможно;
- журналирование действий администраторов — все операции с данными фиксируются для последующего аудита;
- регулярное резервное копирование — обеспечивает восстановление данных в случае сбоя;

- межсетевой экран (firewall) — блокирует несанкционированный сетевой доступ к серверам, разрешая подключение только по разрешённым портам и протоколам;
- антивирусная защита серверного оборудования — предотвращает заражение вредоносным ПО;
- разграничение прав доступа к базам данных (принцип минимальных привилегий) — служебные учётные записи имеют доступ только к тем таблицам и операциям, которые необходимы для их работы.

11. Заключительные положения

11.1. Настоящая Политика является общедоступным документом и размещается на Сайте Оператора.

11.2. Оператор вправе вносить изменения в настоящую Политику. При внесении существенных изменений Оператор размещает соответствующее уведомление на Сайте.

11.3. По всем вопросам, связанным с обработкой персональных данных, просьба обращаться: mds250480@mail.ru.