ПОЛИТИКА
В ОТНОШЕНИИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

платформы MedAccount

ООО «Маркетинговые Технологии» (далее Компания)

Адрес: 108851, Москва г, Щербинка г, Юбилейная ул, дом 20, квартира 95, ИНН: 7722784420, КПП: 775101001, ОГРН: 1127746649689

Версия: 1.0
Дата: 06.04.2026 г.
Статус: утвержден Приказом №1 от 06.04.2026

1. Общие положения

1.1. Настоящая Политика в отношении обработки персональных данных (далее - Политика) определяет принципы, цели, порядок и условия обработки персональных данных, а также сведения о реализуемых требованиях к защите персональных данных при использовании сайтов, личных кабинетов, виджетов, API-интеграций и иных компонентов платформы MedAccount в ООО «Маркетинговые Технологии».

1.2. Политика разработана с учетом Федерального закона от 27.07.2006 N 152-ФЗ "О персональных данных", Федерального закона от 27.07.2006 N 149-ФЗ "Об информации, информационных технологиях и о защите информации", Постановления Правительства РФ от 01.11.2012 N 1119, Приказа ФСТЭК России от 18.02.2013 N 21, Приказа Роскомнадзора от 28.10.2022 N 179, а также иных применимых актов Российской Федерации.

1.3. Политика подлежит опубликованию в свободном доступе на сайте Компании и применяется ко всем персональным данным, которые Компания обрабатывает самостоятельно как оператор либо обрабатывает по поручению клиентов - медицинских организаций.

1.4. Компания оказывает программный сервис для медицинских организаций. В рамках сервиса могут использоваться: сайт, виджет онлайн-записи, личный кабинет пациента, личный кабинет клиники, платформа коммуникаций, интеграция с медицинской информационной системой клиента (МИС) по API, SMS, Telegram, Max и аналитические инструменты.

1.5. Ключевая архитектурная особенность платформы: медицинские данные пациентов не хранятся на серверах Компании. При необходимости отображения медицинской информации сервис в рамках пользовательской сессии обращается к МИС клиента по API, получает необходимые сведения, отображает их на экране уполномоченного пользователя и не сохраняет такие медицинские данные после завершения сессии.

1.6. В уведомлениях пациентам по SMS, Telegram, Max и иным каналам Компания не направляет диагнозы, результаты исследований, назначения, сведения о состоянии здоровья и иные медицинские сведения. Уведомления ограничиваются технической и организационной информацией о записи: подтверждение приема, напоминание о приеме, перенос или отмена записи, предложение нового времени.

2. Термины и определения

Термин	Определение
Автоматизированная обработка персональных данных	обработка персональных данных с помощью средств вычислительной техники.
Биометрические персональные данные	сведения, характеризующие физиологические и биологические особенности человека, на основании которых можно установить его личность и которые используются оператором для установления личности субъекта персональных данных.
Блокирование персональных данных	временное прекращение обработки персональных данных, за исключением случаев, когда обработка необходима для уточнения персональных данных.
Доступ к персональным данным	ознакомление определенных лиц с персональными данными при условии сохранения конфиденциальности таких сведений.
Информационная система персональных данных (ИСПДн)	совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.
Клиент	медицинская организация или иное юридическое лицо, использующее платформу MedAccount на основании договора.
МИС	медицинская информационная система клиента, с которой платформа MedAccount взаимодействует по API.
Обработка персональных данных	любое действие или совокупность действий с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение, извлечение, использование, передачу, предоставление, доступ, обезличивание, блокирование, удаление и уничтожение.
Оператор персональных данных	лицо, самостоятельно или совместно с другими лицами организующее и (или) осуществляющее обработку

	персональных данных, определяющее цели обработки, состав данных и действия с ними.
Обработчик по поручению оператора	лицо, осуществляющее обработку персональных данных по поручению оператора на основании договора или иного поручения, соответствующего требованиям законодательства.
Пациент	физическое лицо, обращающееся в медицинскую организацию, в том числе использующее виджет записи, личный кабинет пациента или каналы уведомлений.
Персональные данные	любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу.
Пользователь платформы	работник, представитель клиента, пациент либо иное лицо, получившее доступ к функциональности MedAccount.
Распространение персональных данных	действия, направленные на раскрытие персональных данных неопределенному кругу лиц.
Специальные категории персональных данных	сведения, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни.
Технические журналы (логи)	записи о событиях в информационных системах, включая дату, время, идентификатор пользователя или сессии, статус запроса, технические параметры, ошибки и иные сведения, необходимые для безопасности, диагностики и контроля работы системы.
Трансграничная передача персональных данных	передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому или иностранному юридическому лицу.
Уничтожение персональных данных	действия, в результате которых становится невозможным восстановить содержание персональных данных в ИСПДн и (или) уничтожаются материальные носители персональных данных.
Файлы cookie	небольшие фрагменты данных, размещаемые на устройстве пользователя для обеспечения работы сайта, сохранения настроек, аналитики и повышения качества сервиса.
Поручение по обработке персональных данных (далее ПОПД)	соглашение (или его часть), в соответствии с которым оператор персональных данных поручает другому лицу (обработчику) осуществлять обработку персональных данных от имени и в интересах оператора на условиях, определенных таким поручением.

3. Роли Компании в обработке персональных данных

3.1. Компания применяет гибридную модель ролей. В зависимости от конкретного процесса Компания может выступать оператором персональных данных, лицом, осуществляющим обработку персональных данных по поручению другого оператора, либо участником совместного процесса обработки при наличии отдельного соглашения.

3.1. Компания как оператор персональных данных

Компания является оператором персональных данных в процессах, где самостоятельно определяет цели, состав данных и операции обработки. К таким процессам относятся:

- прием и обработка заявок с сайта и иных каналов;
- ведение базы лидов, клиентов, партнеров и представителей медицинских организаций;
- создание и сопровождение учетных записей сотрудников и представителей клиник в личном кабинете клиента;
- техническая поддержка пользователей платформы;
- обеспечение информационной безопасности, ведение технических журналов и расследование инцидентов;
- аналитика работы сайта и продукта в пределах, необходимых для развития сервиса и обеспечения качества.

3.2. Компания как обработчик по поручению медицинской организации

При оказании услуг медицинской организации Компания может осуществлять обработку персональных данных пациентов по поручению клиента. В этой части клиент - медицинская организация - является оператором персональных данных пациентов, определяет цели и правовые основания обработки, обеспечивает получение необходимых согласий и исполняет обязанности оператора перед пациентами.

В указанной модели Компания не определяет цели обработки медицинских данных пациентов и не использует такие данные в собственных целях. Действия Компании ограничены договором, поручением на обработку персональных данных, технической документацией и настройками, согласованными с клиентом.

3.3. Обработка медицинских данных без хранения на стороне Компании

Компания не создает и не ведет собственную базу медицинских данных пациентов. При работе функциональности, требующей отображения медицинских сведений, платформа обращается к МИС клиента по API в рамках конкретной сессии и отображает полученные сведения уполномоченному пользователю. После завершения сессии медицинские данные не сохраняются на серверах Компании, не накапливаются и не используются для аналитики или иных целей Компании.

Технические журналы API-запросов ведутся для обеспечения безопасности, диагностики, контроля доступности и расследования инцидентов. В такие журналы не включается содержание медицинских документов, диагнозы, результаты исследований, назначения и иные сведения о состоянии здоровья. Если в исключительной технической ситуации в лог может попасть фрагмент содержательных данных, Компания принимает меры по маскированию, ограничению доступа, сокращенному сроку хранения и последующему удалению таких сведений.

4. Принципы обработки персональных данных

4.1. Компания обрабатывает персональные данные на законной и справедливой основе, строго в пределах заранее определенных и законных целей.

- не допускается обработка персональных данных, несовместимая с целями их сбора;
- состав и объем данных должны соответствовать заявленным целям обработки;
- не допускается избыточная обработка персональных данных;
- обеспечивается точность, достаточность и актуальность данных;

- хранение данных осуществляется не дольше, чем требуется для целей обработки, если иной срок не установлен законом или договором;
- по достижении целей обработки или при наступлении иных оснований данные подлежат уничтожению, обезличиванию или возврату оператору, если применимо;
- доступ к данным предоставляется только лицам, которым он необходим для выполнения обязанностей;
- медицинские данные пациентов не используются Компанией для собственных целей и не хранятся на серверах Компании.

5. Цели обработки, категории субъектов и категории персональных данных

5.1. Перечень процессов обработки персональных данных приведен в Приложении 1 к Политике. Для каждого процесса определены цель, категории субъектов, состав данных, способы обработки, правовые основания, сроки хранения и порядок уничтожения.

5.2. Компания обрабатывает следующие основные категории субъектов: посетители сайта, лица, оставляющие заявки, клиенты и представители клиентов, сотрудники и пользователи клиентов, пациенты клиентов, пользователи платформы, контрагенты и представители контрагентов, лица, обращающиеся в службу поддержки.

5.3. Компания не осуществляет обработку биометрических персональных данных для установления личности субъектов.

5.4. Специальные категории персональных данных, относящиеся к состоянию здоровья пациентов, могут временно отображаться в рамках API-сессии по поручению медицинской организации. Компания не хранит такие сведения на своих серверах и не включает их в уведомления, аналитику, технические журналы и продуктовые отчеты.

6. Правовые основания обработки

6.1. В зависимости от процесса Компания обрабатывает персональные данные на одном или нескольких правовых основаниях:

- согласие субъекта персональных данных;
- исполнение договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных;
- заключение договора по инициативе субъекта;
- исполнение обязанностей, возложенных законодательством Российской Федерации;
- осуществление прав и законных интересов Компании, клиента или третьих лиц при условии, что не нарушаются права и свободы субъекта;
- обработка по поручению оператора - медицинской организации - в пределах договора и поручения.

6.2. При обработке данных пациентов по поручению клиента правовое основание отношений с пациентом определяет медицинская организация. Компания обеспечивает обработку в пределах поручения и не подменяет собой оператора персональных данных пациента.

7. Поручение обработки персональных данных

7.1. В части обработки персональных данных пациентов и иных данных, переданных клиентом, Компания действует по поручению клиента, если иное прямо не предусмотрено договором или законом.

7.2. Поручение обработки персональных данных включается в договор с клиентом, приложение к договору, ПОПД, техническое задание, регламент интеграции либо иной документ, позволяющий определить:

- перечень персональных данных;
- категории субъектов персональных данных;
- цели обработки;

- перечень действий с персональными данными;
- требования к защите персональных данных;
- порядок привлечения субобработчиков;
- порядок возврата, удаления или прекращения обработки данных;
- порядок взаимодействия при запросах субъектов и инцидентах безопасности.

7.3. При обработке по поручению Компания обязуется:

- обрабатывать персональные данные только в пределах поручения клиента;
- не использовать данные пациентов для собственных маркетинговых, аналитических или иных самостоятельных целей;
- обеспечивать конфиденциальность персональных данных;
- принимать необходимые правовые, организационные и технические меры защиты;
- обеспечивать хранение инфраструктуры в Российской Федерации в части собственных серверов и баз данных Компании;
- не сохранять медицинские данные пациентов на серверах Компании после завершения пользовательской сессии;
- обеспечивать, чтобы уведомления пациентам не содержали диагнозов, результатов исследований, назначений и иных медицинских сведений;
- уведомлять клиента об инцидентах безопасности в порядке и сроки, предусмотренные договором и законом.

7.4. Клиент, действующий как оператор персональных данных пациентов, отвечает за законность сбора персональных данных пациентов, информирование пациентов, получение необходимых согласий, определение состава данных, передаваемых через API, и предоставление Компании поручения, соответствующего требованиям законодательства.

8. Порядок и условия обработки персональных данных

8.1. Компания осуществляет автоматизированную, неавтоматизированную и смешанную обработку персональных данных, с передачей данных по информационно-телекоммуникационным сетям или без такой передачи.

8.2. Обработка может включать сбор, запись, систематизацию, накопление, хранение, уточнение, извлечение, использование, передачу, предоставление, доступ, блокирование, удаление, уничтожение, а в предусмотренных случаях - обезличивание.

8.3. Сбор, запись, систематизация, накопление, хранение, уточнение и извлечение персональных данных граждан Российской Федерации, обрабатываемых в собственных информационных системах Компании, обеспечиваются с использованием баз данных, находящихся на территории Российской Федерации.

8.4. Хостинг и основные серверные мощности Компании размещаются на территории Российской Федерации. Интеграция с МИС клиента осуществляется по защищенным каналам связи на основании технических настроек и прав доступа, согласованных с клиентом.

8.5. Доступ работников и подрядчиков Компании к персональным данным предоставляется по принципу минимально необходимых прав. Доступ фиксируется и пересматривается при изменении должностных обязанностей, завершении проекта или прекращении отношений.

9. Уведомления пациентам и коммуникационные каналы

9.1. В рамках платформы могут направляться сервисные уведомления пациентам по SMS, Telegram, Max и иным каналам, выбранным пациентом или медицинской организацией.

9.2. Содержание уведомлений ограничивается организационной информацией: подтверждение записи, напоминание о приеме, перенос записи, отмена записи, предложение нового времени, техническая ссылка или код подтверждения.

9.3. В уведомления не включаются диагнозы, результаты анализов и исследований, врачебные назначения, сведения о состоянии здоровья, медицинские документы и иная медицинская информация.

9.4. Если выбранный канал коммуникации предполагает передачу данных третьему лицу или трансграничную передачу, такая передача ограничивается минимальным набором данных, необходимым для доставки уведомления. Медицинские данные через такие каналы не передаются.

10. Субобработчики и третьи лица

10.1. Компания может привлекать третьих лиц и субобработчиков для обеспечения работы платформы, если это необходимо для оказания услуг, обеспечения безопасности, доставки уведомлений, размещения инфраструктуры, аналитики или технической поддержки.

10.2. К типовым категориям субобработчиков относятся:

- провайдеры хостинга и облачной инфраструктуры на территории Российской Федерации;
- операторы SMS и иных сервисных сообщений;
- платформы мессенджеров, включая Telegram и Max, при выборе соответствующего канала коммуникации;
- провайдеры аналитики сайта и продукта;
- поставщики средств мониторинга, журналирования, антифрода, защиты от атак и резервного копирования;
- подрядчики технической поддержки и разработки, имеющие доступ только к минимально необходимым данным.

10.3. Субобработчики привлекаются на основании договоров или иных юридически значимых документов, предусматривающих конфиденциальность, требования к защите данных, ограничения целей обработки, запрет несанкционированного распространения и ответственность за нарушение обязательств.

10.4. При обработке по поручению клиента порядок привлечения субобработчиков определяется договором с клиентом (в т.ч. договором оферты) или ПОПД. Компания не передает субобработчикам медицинские данные пациентов для хранения, аналитики или самостоятельного использования.

11. Трансграничная передача персональных данных

11.1. В общем случае Компания стремится минимизировать трансграничную передачу персональных данных. Основная инфраструктура и базы данных Компании размещаются на территории Российской Федерации.

11.2. Трансграничная передача может возникать при использовании отдельных коммуникационных каналов или сервисов, включая мессенджеры, если техническая архитектура соответствующего сервиса предполагает обработку данных за пределами Российской Федерации.

11.3. В случае трансграничной передачи Компания обеспечивает соблюдение применимых требований законодательства, включая оценку допустимости такой передачи, минимизацию состава передаваемых данных, информирование субъектов и (при необходимости) получение согласий либо иное законное основание.

11.4. Медицинские данные пациентов, включая диагнозы, назначения, результаты исследований и сведения о состоянии здоровья, не передаются через Telegram, Max, SMS и иные каналы уведомлений.

12. Cookies и аналитика

12.1. Сайт и веб-интерфейсы Компании могут использовать cookies, пиксели, локальное хранилище браузера, идентификаторы сессии и аналогичные технологии.

12.2. Cookies используются для следующих целей:

- обеспечение работоспособности сайта, виджета и личного кабинета;
- аутентификация и сохранение сессии пользователя;
- обеспечение безопасности, предотвращение злоупотреблений и технических сбоев;
- сохранение пользовательских настроек;
- сбор обезличенной или агрегированной статистики посещений и использования функциональности;
- улучшение интерфейса, качества сервиса и продуктовой аналитики.

12.3. Компания может использовать аналитические сервисы, включая Яндекс.Метрику, собственную аналитику и иные сервисы, перечень которых подлежит раскрытию на сайте или в интерфейсе сервиса. Аналитика не должна включать медицинские данные пациентов.

12.4. Пользователь может ограничить или отключить cookies в настройках браузера. Отключение обязательных cookies может привести к недоступности отдельных функций сайта, виджета или личного кабинета.

12.5. Сведения, полученные с использованием аналитических инструментов, используются в обезличенном или агрегированном виде, если иное прямо не предусмотрено законным основанием и не требуется для обеспечения безопасности или исполнения договора оферты.

13. Логирование, мониторинг и API-интеграция с МИС

13.1. Компания ведет технические журналы событий для обеспечения безопасности, диагностики ошибок, контроля доступности, учета действий пользователей, расследования инцидентов и подтверждения фактов обработки.

13.2. При интеграции с МИС клиента в логах могут фиксироваться: дата и время запроса, идентификатор клиента, идентификатор пользователя или сессии, технический идентификатор запроса, тип операции или endpoint, код ответа, статус выполнения, сведения об ошибке, IP-адрес, user-agent, сведения о версии интеграции.

13.3. В технические журналы не должны включаться медицинские документы, диагнозы, результаты исследований, назначения и иные сведения о состоянии здоровья. Компания применяет маскирование, фильтрацию, ограничение прав доступа и сокращенные сроки хранения для журналов повышенной чувствительности.

13.4. Доступ к API МИС осуществляется по защищенным каналам связи, с применением механизмов аутентификации, авторизации и разграничения прав. Параметры интеграции определяются договором оферты, технической документацией и настройками клиента.

14. Сроки хранения, прекращение обработки и уничтожение

14.1. Сроки хранения персональных данных определяются целями обработки, договором оферты, требованиями законодательства и реестром процессов обработки, приведенным в Приложении 1.

14.2. Медицинские данные пациентов, временно получаемые по API из МИС клиента для отображения в рамках сессии, не хранятся на серверах Компании после завершения сессии.

14.3. Обработка персональных данных прекращается при достижении целей обработки, истечении срока хранения, отзыве согласия, прекращении договора оферты, получении законного требования субъекта или оператора, выявлении неправомерной обработки либо наступлении иных оснований, предусмотренных законом.

14.4. Уничтожение персональных данных осуществляется способом, исключающим возможность восстановления содержания данных. Для бумажных носителей используется уничтожение, исключающее восстановление; для электронных данных - удаление средствами информационной системы, криптографическое стирание, перезапись, удаление резервных копий по установленному циклу либо иные применимые методы.

14.5. Подтверждение уничтожения осуществляется в соответствии с применимыми требованиями Роскомнадзора: актом об уничтожении, выгрузкой из журнала регистрации событий или иными документами, предусмотренными внутренними регламентами и законом.

15. Права субъектов персональных данных

15.1. Субъект персональных данных вправе получать сведения об обработке своих персональных данных, требовать уточнения, блокирования или уничтожения данных, отзывать согласие, обжаловать действия или бездействие оператора в уполномоченный орган или суд, а также реализовывать иные права, предусмотренные законом.

15.2. Запрос субъекта должен позволять идентифицировать субъекта и факт его отношений с Компанией или клиентом. Запрос может быть направлен по адресу Компании, через электронные каналы, указанные на сайте, либо через медицинскую организацию, если обработка осуществляется по ее поручению.

15.3. Если запрос относится к данным пациента, обрабатываемым Компанией по поручению медицинской организации, Компания вправе перенаправить запрос клиенту или действовать по его указанию, если иное не предусмотрено законом или договором оферты.

15.4. Ответы на запросы субъектов предоставляются в сроки, предусмотренные законодательством Российской Федерации. При необходимости срок может быть продлен в случаях и порядке, допускаемых законом.

16. Меры по обеспечению безопасности персональных данных

16.1. Компания принимает необходимые правовые, организационные и технические меры для защиты персональных данных от неправомерного или случайного доступа, уничтожения, изменения, блокирования, копирования, предоставления, распространения и иных неправомерных действий.

16.1. Правовые меры

- утверждение Политики и внутренних регламентов обработки персональных данных;
- заключение договоров, соглашений о конфиденциальности и поручений обработки персональных данных;
- определение ролей сторон в договоре оферты с клиентами и субобработчиками;
- регламентация доступа работников и подрядчиков к персональным данным;
- ведение и актуализация реестра процессов обработки.

16.2. Организационные меры

- назначение лица, ответственного за организацию обработки персональных данных;
- назначение лиц, ответственных за обеспечение безопасности персональных данных в информационных системах;
- ознакомление работников с требованиями законодательства, Политикой и внутренними регламентами;
- обучение работников правилам обработки и защиты персональных данных;
- ограничение круга лиц, имеющих доступ к персональным данным;
- разделение ролей и прав доступа по принципу минимально необходимого доступа;
- периодический пересмотр прав доступа;
- учет носителей персональных данных;
- регламентация действий при инцидентах информационной безопасности;
- контроль подрядчиков и субобработчиков.

16.3. Технические меры

- идентификация и аутентификация пользователей;
- разграничение доступа к системам и данным;

- использование защищенных каналов передачи данных;
- защита API и контроль авторизации запросов;
- ведение журналов событий безопасности и действий пользователей;
- мониторинг доступности и аномальной активности;
- резервное копирование и проверка восстановления;
- антивирусная защита и защита от вредоносного кода;
- межсетевое экранирование и сегментация инфраструктуры;
- управление уязвимостями и обновлениями;
- защита секретов, токенов и ключей доступа;
- маскирование или исключение медицинских данных из логов;
- ограничение доступа к production-данным для разработки и тестирования.

16.4. Уровни защищенности ИСПДн

Компания определяет уровни защищенности персональных данных в ИСПДн в соответствии с Постановлением Правительства РФ N 1119 с учетом категорий обрабатываемых персональных данных, количества субъектов, актуальных угроз и характера обработки.

Для процессов, где Компания является оператором и обрабатывает преимущественно контактные, учетные и технические данные пользователей, применимый уровень защищенности определяется по результатам внутренней классификации ИСПДн и модели угроз. Для процессов, в которых временно отображаются специальные категории персональных данных пациентов по поручению медицинской организации без хранения на серверах Компании, уровень защищенности и состав мер определяются с учетом характера сессионной обработки, отсутствия накопления медицинских данных и условий договора оферты с клиентом.

Конкретный набор мер безопасности определяется внутренними документами Компании, моделью угроз, результатами оценки вреда субъектам персональных данных, архитектурой ИСПДн и требованиями применимых нормативных актов, включая Приказ ФСТЭК России N 21.

17. Инциденты безопасности

17.1. Компания принимает меры по выявлению, регистрации, анализу, локализации и устранению инцидентов, связанных с нарушением безопасности персональных данных.

17.2. При инциденте Компания определяет характер инцидента, категории затронутых данных, круг затронутых субъектов, возможные последствия, меры локализации, необходимость уведомления клиентов, субъектов, уполномоченных органов и иных лиц.

17.3. Если инцидент относится к данным, обрабатываемым по поручению клиента, Компания уведомляет клиента в порядке, установленном договором оферты, и оказывает разумное содействие в исполнении обязанностей оператора.

18. Заключительные положения

18.1. Политика вступает в силу с даты ее утверждения и действует до замены новой редакцией.

18.2. Политика пересматривается при изменении законодательства, архитектуры платформы, состава процессов обработки, перечня субобработчиков, каналов коммуникации, условий хранения данных либо при выявлении необходимости актуализации по результатам аудита или инцидента.

18.3. Актуальная редакция Политики размещается на сайте Компании. По вопросам обработки персональных данных можно обратиться по адресу: info@medaccount.ru .

Приложение 1. Реестр процессов обработки персональных данных

Реестр является частью Политики и отражает ключевые процессы обработки персональных данных в рамках платформы MedAccount. Конкретный состав данных может уточняться договором оферты, поручением обработки, технической документацией, формами согласий и настройками клиента.

N	Процесс / цель обработки	Роль Компании	Категории субъектов	Категории и перечень ПД	Способ и операции обработки	Правовое основание	Срок хранения / обработки	Порядок уничтожения / прекращения
1	Обработка заявок на сайте, входящих обращений и запросов на демонстрацию сервиса	Оператор	Посетители сайта; представители медицинских организаций; потенциальные клиенты	ФИО; должность; организация; телефон; email; содержание обращения; сведения о выбранном канале связи; технические данные формы	Автоматизированная и смешанная обработка: сбор, запись, систематизация, хранение, уточнение, использование, предоставление доступа ответственным сотрудникам, удаление	Согласие субъекта; заключение договора по инициативе субъекта; законный интерес Компании в обработке обращения	До достижения цели обращения, но не более 3 лет с последнего контакта, если более длительный срок не требуется для договора, спора или закона	Удаление из CRM и почтовых систем; обезличивание аналитических сведений; акт или системная запись об удалении при применимости
2	Ведение договорной работы с клиентами и партнерами	Оператор	Клиенты; представители клиентов; контрагенты; представители контрагентов	ФИО; должность; организация; телефон; email; доверенности; полномочия; подпись; реквизиты документов в случаях, необходимых для договора; деловая переписка	Смешанная обработка: сбор, хранение, использование, передача в бухгалтерские, юридические и банковские системы, архивирование, уничтожение	Исполнение договора; заключение договора; исполнение требований закона; законный интерес в защите прав	Срок договора и сроки исковой давности; бухгалтерские и юридически значимые документы - в сроки, установленные законом	Архивное хранение до истечения обязательных сроков; затем уничтожение бумажных носителей и удаление электронных копий
3	Создание и администрирование личного кабинета клиента (клиники)	Оператор	Сотрудники и представители клиентов; пользователи платформы со стороны клиники	ФИО; email; телефон; должность; роль в системе; логин; идентификатор пользователя; история входов; настройки доступа; сведения об организации	Автоматизированная обработка: создание учетной записи, хранение, уточнение, предоставление доступа, блокирование, удаление	Исполнение договора с клиентом; законный интерес в обеспечении безопасности; поручение клиента в части управления пользователями клиента	На срок действия договора с клиентом и до 180 дней после прекращения доступа, если иной срок не установлен договором или законом	Блокирование учетной записи; удаление или обезличивание профиля; сохранение минимальных логов безопасности на установленный срок
4	Предоставление доступа пациенту к виджету записи и личному кабинету пациента	В зависимости от процесса: обработчик по поручению клиники; оператор для собственных технических данных	Пациенты клиентов; законные представители пациентов при применимости	ФИО; телефон; email; дата рождения; пол; идентификатор записи; выбранная клиника, врач, услуга, дата и время приема; технические данные сессии	Автоматизированная обработка: сбор, запись, передача в МИС клиента, отображение в интерфейсе, предоставление доступа, удаление	Поручение медицинской организации; согласие субъекта или иное основание, определенное клиникой; исполнение договора между клиникой и пациентом	Данные записи - в пределах срока, установленного клиентом и договором; технические сессионные данные - в срок, необходимый для работы сервиса и безопасности	Передача в МИС клиента; удаление из временных областей; удаление или обезличивание технических данных по истечении срока
5	API-взаимодействие с МИС клиента для отображения медицинской информации	Обработчик по поручению клиники	Пациенты клиентов; уполномоченные пользователи клиники	Медицинские данные, получаемые из МИС клиента только в объеме, необходимом для отображения в рамках сессии; идентификаторы пациента, записи, врача или документа; содержательные медицинские данные не сохраняются на серверах Компании	Автоматизированная сессионная обработка: запрос по API, получение, временное отображение, передача ответа в интерфейс, прекращение обработки после завершения сессии	Поручение медицинской организации; правовое основание обработки определяется клиникой как оператором данных пациента	Медицинские данные не хранятся на серверах Компании после завершения сессии; технические сведения о запросах хранятся в логах без содержания медицинских данных	Прекращение сессии; очистка временных данных; запрет записи содержательных медицинских данных в постоянные хранилища; удаление логов по срокам хранения
6	Направление сервисных уведомлений пациентам о записи	Обработчик по поручению клиники; оператор в части технической доставки сообщений при применимости	Пациенты клиентов	Телефон; идентификатор канала; имя или обращение при необходимости; дата и время приема; факт записи, переноса или отмены; ссылка или код подтверждения; без	Автоматизированная обработка: формирование сообщения, передача SMS-провайдеру или мессенджеру, фиксация статуса доставки	Поручение клиники; согласие субъекта на коммуникации или иное основание, определенное клиникой; исполнение договора с клиентом	Статусы доставки и технические сведения - до 1 года, если иной срок не установлен договором или законом	Удаление статусов и очередей сообщений; хранение агрегированной статистики без идентификации субъекта

				диагнозов, результатов, назначений и иных медицинских сведений				
7	Использование Telegram, Max и иных мессенджеров для уведомлений	Обработчик по поручению клиники; оператор в части выбора и настройки канала в собственном сервисе	Пациенты, выбравшие соответствующий канал; пользователи платформы	Идентификатор мессенджера; телефон или username при наличии; технический идентификатор диалога; минимальная информация о записи без медицинских данных	Автоматизированная обработка: привязка канала, направление сервисных сообщений, получение статусов доставки, отключение канала	Согласие субъекта на выбранный канал; поручение клиники; исполнение договора; законный интерес в доставке сервисных сообщений	До отключения канала, отзыва согласия или прекращения договора; технические статусы - до 1 года	Удаление привязки канала и токенов; удаление очередей сообщений; обезличивание статистики
8	Техническая поддержка пользователей платформы	Оператор; обработчик по поручению клиента, если обращение содержит данные пациента	Сотрудники клиентов; представители клиентов; пациенты; иные пользователи	ФИО; контактные данные; организация; роль; содержание обращения; скриншоты или вложения; технические данные устройства; идентификаторы сессии; при случайном получении медицинских данных - ограниченная обработка для решения обращения	Смешанная обработка: прием обращения, регистрация тикета, анализ, ответ, хранение истории поддержки, удаление	Исполнение договора; согласие при обращении; законный интерес в поддержке и безопасности; поручение клиники в части данных пациентов	До 3 лет после закрытия обращения, если иной срок не установлен договором; данные повышенной чувствительности удаляются раньше при отсутствии необходимости	Удаление тикетов и вложений; маскирование чувствительных фрагментов; обезличивание базы знаний
9	Ведение технических журналов, мониторинг и обеспечение информационной безопасности	Оператор; обработчик в части событий, относящихся к данным клиента	Пользователи сайта; пользователи платформы; сотрудники клиентов; пациенты в части технических идентификаторов	IP-адрес; user-agent; дата и время; идентификатор пользователя, клиента, сессии или запроса; endpoint; статус ответа; ошибки; действия пользователя; без содержания медицинских документов	Автоматизированная обработка: запись, хранение, анализ, корреляция событий, ограниченное предоставление доступа администраторам безопасности, удаление	Законный интерес в безопасности; исполнение договора; требования закона; поручение клиента	Обычно до 12 месяцев, если иной срок не требуется для расследования инцидента, спора или закона	Удаление средствами журналирования; ротация логов; обезличивание; ограничение доступа к архивам
10	Аналитика сайта и продукта, cookies	Оператор	Посетители сайта; пользователи виджета; пользователи платформы	Cookie ID; IP-адрес; сведения о браузере и устройстве; источник перехода; действия на сайте; события интерфейса; агрегированные показатели; без медицинских данных	Автоматизированная обработка: сбор cookies, запись событий, агрегация, обезличивание, анализ, удаление	Согласие при необходимости; законный интерес в улучшении сервиса и безопасности; настройки браузера пользователя	До 24 месяцев либо срок, установленный используемым аналитическим сервисом; агрегированные данные могут храниться дольше без идентификации субъекта	Удаление cookie-идентификаторов; обезличивание; отключение аналитики по запросу или настройкам браузера
11	Рассылка информационных и маркетинговых сообщений представителям клиник	Оператор	Представители клиентов; потенциальные клиенты; партнеры	ФИО; должность; организация; телефон; email; история коммуникаций; предпочтения по коммуникации	Автоматизированная и смешанная обработка: сегментация, направление сообщений, учет отказов, удаление	Согласие; законный интерес при B2B-коммуникации в допустимых пределах; исполнение договора	До отказа от рассылки, отзыва согласия или утраты актуальности контакта; не более 3 лет без подтверждения актуальности	Исключение из рассылки; удаление или архивирование контакта; фиксация отказа в стоп-листе
12	Исполнение запросов субъектов персональных данных	Оператор; обработчик по поручению клиента	Субъекты ПД; представители субъектов; клиенты	ФИО; контактные данные; сведения, подтверждающие полномочия; содержание запроса; ответ на запрос; история действий по запросу	Смешанная обработка: прием, идентификация, проверка, подготовка ответа, направление ответа, хранение подтверждения исполнения	Исполнение требований закона; законный интерес в подтверждении исполнения обязанностей	Срок рассмотрения и хранения материалов запроса - обычно до 3 лет для подтверждения исполнения обязанностей или защиты прав	Удаление материалов запроса по истечении срока; уничтожение бумажных копий
13	Рассмотрение претензий, досудебная и судебная защита прав	Оператор	Клиенты; представители клиентов; пользователи; пациенты; контрагенты	ФИО; контактные данные; договорные документы; переписка; сведения о споре; технические журналы; доказательства действий в системе	Смешанная обработка: сбор, анализ, хранение, передача юристам, суду, госорганам, архивирование, уничтожение	Законный интерес в защите прав; исполнение договора; требования закона	В течение срока спора, сроков исковой давности и обязательного хранения документов	Архивирование до окончания срока; затем уничтожение или обезличивание

Приложение 2. Матрица ролей и ответственности

Сценарий	Роль MedAccount	Роль клиники	Ключевая ответственность
Заявка на сайте MedAccount	Оператор	Не участвует	MedAccount определяет цели обработки заявки, отвечает на обращение, ведет CRM и обеспечивает защиту данных.
Личный кабинет клиники: сотрудники клиники	Оператор в части учетных записей; возможно обработчик в части настроек клиента	Клиника определяет сотрудников и их роли	MedAccount обеспечивает учетные записи, разграничение доступа и техническую безопасность. Клиника отвечает за актуальность пользователей и своевременное отключение доступа.
Запись пациента через виджет	Обработчик по поручению клиники в части пациентских данных; оператор в части технических логов	Оператор данных пациента	Клиника определяет цели и основания обработки пациента. MedAccount обеспечивает техническую передачу и интерфейс.
Отображение медицинских данных из МИС	Обработчик без хранения медданных	Оператор медицинских данных	MedAccount обращается к МИС по API в рамках сессии и не сохраняет медицинские данные после ее завершения.
SMS / Telegram / Max уведомления	Обработчик доставки уведомлений по поручению клиники	Оператор коммуникации с пациентом	Передаются только минимальные сведения о записи; медицинская информация не передается.
Аналитика сайта	Оператор	Не участвует	MedAccount собирает обезличенную или агрегированную аналитику без медицинских данных.

Приложение 3. Политика cookies и аналитики для публикации на сайте

Сайт MedAccount использует cookies и аналитические технологии для обеспечения работы сайта, защиты от злоупотреблений, сохранения пользовательских настроек, анализа посещаемости и улучшения качества сервиса. Продолжая использовать сайт, пользователь соглашается с применением cookies, если такое согласие требуется применимым законодательством и интерфейсом сайта.

Типы cookies:

- обязательные cookies - нужны для работы сайта, виджета и личного кабинета;
- функциональные cookies - сохраняют настройки и предпочтения;
- аналитические cookies - помогают понимать, как используется сайт и продукт;
- cookies безопасности - помогают предотвращать злоупотребления, атаки и несанкционированный доступ.

В аналитические инструменты не передаются медицинские данные пациентов. Пользователь может изменить настройки cookies в браузере; при отключении обязательных cookies часть функций может работать некорректно.

Приложение 4. Нормативные источники, учтенные при подготовке Политики

- Федеральный закон от 27.07.2006 N 152-ФЗ "О персональных данных".
- Федеральный закон от 27.07.2006 N 149-ФЗ "Об информации, информационных технологиях и о защите информации".
- Постановление Правительства РФ от 01.11.2012 N 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных".

- Приказ ФСТЭК России от 18.02.2013 N 21 "Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных".
- Приказ Роскомнадзора от 28.10.2022 N 179 "Об утверждении требований к подтверждению уничтожения персональных данных".

Приложение 5. Категории субобработчиков и минимальные договорные требования

Настоящее приложение описывает подход Компании к привлечению субобработчиков. Конкретный перечень юридических лиц, их реквизиты и страны обработки рекомендуется вести в отдельном актуализируемом реестре субобработчиков и раскрывать клиентам в порядке, установленном договором или ПОПД.

Категория субобработчика	Типовые задачи	Передаваемые данные	Ограничения	Минимальные договорные требования
Хостинг и дата-центр в РФ	Размещение серверов, резервное копирование, сетевые сервисы	Инфраструктурные данные, базы приложения, учетные и технические данные; медицинские данные пациентов не хранятся	Размещение основных баз данных на территории РФ; доступ персонала дата-центра ограничивается	Конфиденциальность; меры защиты; доступ только при необходимости; уведомление об инцидентах; запрет самостоятельного использования данных
SMS-провайдер	Доставка сервисных уведомлений пациентам и пользователям	Номер телефона; текст сервисного уведомления без медицинских сведений; статус доставки	Запрет передачи диагнозов, результатов, назначений и иных сведений о здоровье	Обработка только для доставки; сроки хранения статусов; защита каналов; удаление очередей сообщений; ответственность за нарушения
Telegram / Max и иные мессенджеры	Доставка уведомлений при выборе соответствующего канала	Идентификатор канала; телефон или username; технические статусы; минимальная информация о записи без медицинских данных	Использование только при наличии выбранного канала и законного основания; минимизация данных	Информирование о возможной трансграничной обработке; запрет медицинского содержания; возможность отключения канала
Аналитические сервисы	Статистика сайта, продуктовая аналитика, улучшение UX	Cookie ID; IP; user-agent; события интерфейса; агрегированные данные	Запрет передачи медицинских данных и содержимого медицинских документов	Обезличивание/агрегация; настройка сроков хранения; режим конфиденциальности; отключение по настройкам
Сервисы мониторинга и безопасности	Мониторинг доступности, ошибок, атак, событий безопасности	Технические журналы; IP; идентификаторы сессий; сведения об ошибках без медицинских данных	Фильтрация чувствительных данных; ограничение доступа к логам	Режим конфиденциальности; управление доступом; сроки хранения; уведомление об инцидентах; удаление по окончании необходимости
Подрядчики разработки и технической поддержки	Разработка, сопровождение, устранение ошибок	Тестовые данные, обезличенные данные, технические сведения; production-доступ только при необходимости	Запрет использования реальных медицинских данных в тестовых средах; доступ по заявке	NDA; минимальный доступ; журналирование действий; запрет копирования данных; возврат/удаление после работ

Приложение 6. Процедура реагирования на запросы субъектов и инциденты

1. Запросы субъектов персональных данных

Компания разделяет запросы по принадлежности процесса: собственная обработка Компании как оператора и обработка по поручению клиента. Если запрос относится к пациентским данным клиники, Компания действует совместно с клиентом и не принимает самостоятельных решений о раскрытии, изменении или удалении медицинских данных, если иное не установлено законом.

- зарегистрировать запрос и канал поступления;
- идентифицировать субъекта или его представителя в допустимом объеме;
- определить процесс обработки и роль Компании;
- если Компания является оператором - подготовить ответ и выполнить законное требование;
- если Компания является обработчиком - уведомить клиента и действовать по его поручению;
- зафиксировать результат исполнения запроса и срок ответа.

2. Инциденты безопасности

При обнаружении события, которое может повлечь нарушение конфиденциальности, целостности или доступности персональных данных, Компания инициирует процедуру реагирования.

- первичная фиксация события и его классификация;
- локализация инцидента и предотвращение дальнейшего распространения;
- определение затронутых систем, категорий данных и субъектов;
- проверка, затронуты ли медицинские данные пациентов или только технические идентификаторы;
- уведомление клиента, если инцидент относится к обработке по поручению;
- подготовка уведомлений уполномоченным органам и субъектам, если такая обязанность возникает;
- устранение причин инцидента и документирование принятых мер;
- пост-инцидентный анализ и корректировка мер защиты.

3. Контрольные сроки и документы

Событие	Документирование	Ответственный процесс
Запрос субъекта	Журнал запросов, копия ответа, подтверждение отправки	Ответственный за организацию обработки ПД
Запрос клиента-оператора	Тикет/служебная запись, поручение клиента, результат исполнения	Ответственный менеджер и ИБ
Инцидент ИБ	Карточка инцидента, журнал событий, план реагирования, отчет о причинах	Ответственный за ИБ
Уничтожение данных	Акт, выгрузка из журнала или иной документ подтверждения	Владелец процесса и ИБ