ЧАСТЬ А. РЕГЛАМЕНТ СЕРВИСА

К Пользовательскому соглашению (часть А — регламент сервиса) и Политике обработки персональных данных (часть В) · редакция от 30.09.2026

А1. Термины и определение Сервиса

1.1. **Сервис «Защищённая связь»** (далее — «Сервис») — функциональный модуль Экосистемы Gramaton, обеспечивающий защищённый канал связи и коммуникаций Пользователей: сквозное шифрование переписки в личных чатах, защищённый раздел «Закрытые чаты», защиту вложений, защиту исходящего контента от копирования и снятия экрана получателем, управление доверенными устройствами и сессиями, локальную защиту данных на устройстве, а также фиксацию событий безопасности Сервиса.

1.2. **Сквозное шифрование (E2EE, end-to-end encryption)** — шифрование сообщений на устройстве отправителя и расшифрование на устройстве получателя. Криптографические операции выполняются **только на устройствах Пользователей**; Оператор не выполняет шифрование и расшифрование переписки и не располагает ключами для её чтения.

1.3. **Устройство** — клиент (мобильное приложение, веб-клиент), зарегистрированный в Сервисе для работы с E2EE. Устройство имеет собственную пару ключей; **приватные ключи не покидают устройство**.

1.4. **Конверт (envelope)** — непрозрачный для Оператора блок зашифрованных данных, которому адресовано конкретное сообщение конкретного Устройства получателя. Оператор хранит и передаёт конверты, не разбирая их содержимое.

1.5. **Закрытые чаты** — защищённый раздел Сервиса: переписка с выбранными Пользователем контактами, для которой шифрование применяется **обязательно**, раздел скрыт из общего списка чатов и поиска и открывается только после ввода PIN-кода (см. А3).

1.6. **Защита исходящего контента** — режим, при котором сообщения Пользователя, имеющего активную подписку (см. А4), помечаются для получателя как защищённые: на стороне получателя блокируются копирование, сохранение, пересылка, скачивание вложений, а экран чата защищается от снятия скриншотов средствами операционной системы, пока такие сообщения отображаются.

1.7. **Журнал безопасности** — доступный Пользователю перечень событий безопасности его аккаунта в Сервисе (подключение и отключение устройств, регистрация ключей, отчёты о невозможности расшифрования и т.п.) без раскрытия ключевого материала и содержимого переписки.

1.8. **Участники:** Оператор и Пользователи. Роли Пользователей в Сервисе: **отправитель** и **получатель** сообщений; специальных ролей (заказчик/исполнитель/перевозчик/продавец) Сервис не вводит.

1.9. **Тайна связи и переписки.** Оператор обеспечивает конфиденциальность сведений, передаваемых Пользователями в Сервисе, руководствуясь ст. 22–24 Конституции РФ, ст. 63 Федерального закона от 07.07.2003 № 126-ФЗ «О связи» (для лиц, на которых распространяется режим тайны связи), Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» и Политикой обработки ПД. Доступ третьих лиц к сведениям о переписке — только в случаях и в порядке, установленных законом.

1.10. **Сервис не является** и Оператор в рамках Сервиса **не осуществляет**: оказание услуг связи, деятельность оператора связи или оператора подвижной радиотелефонной связи; продажу товаров, выполнение работ, оказание бытовых или иных услуг Пользователям; банковскую деятельность; предоставление средств обхода установленных законом ограничений доступа к информационным ресурсам.

1.11. **Сервис не является** хранилищем «резервных копий переписки»: Оператор не формирует облачных копий содержимого защищённой переписки (см. А6.4, В10).

1.12. **Границы Сервиса.** Сервис регулирует **защитные функции коммуникаций**. Условия обмена сообщениями как такового (регистрация контактов, группы, реакции, подарки, модерация контента) устанавливаются Приложением о сервисе «Мессенджер»; обработка персональных данных в этом объёме — Политикой обработки ПД и указанным Приложением. Настоящее Приложение применяется к Сервису в части защищённого канала и защиты данных.

A2. Роли сторон и правовое положение Оператора

2.1. Оператор — правообладатель программного обеспечения, владелец информационной инфраструктуры и **лицо, организующее информационное взаимодействие** между Пользователями (Пользовательское соглашение, п. 2.3).

2.2. Оператор является **информационным посредником** в смысле ст. 1253.1 Гражданского кодекса РФ и не определяет содержание передаваемых Пользователями сообщений, не редактирует их и не является их автором.

2.3. Оператор **не является** оператором связи, стороной правоотношений между Пользователями, оператором платёжных услуг, а также лицом, обязанным обеспечить защиту от любых действий третьих лиц на устройстве Пользователя (см. A6.4).

2.4. Оператор обеспечивает **техническую** защиту канала и серверной части Сервиса в объёме принятых мер (Часть B, раздел B8) и **не гарантирует** защищённость устройства Пользователя, его учётных данных, пароля/PIN-кода и кода доступа, а также невозможность снятия экрана камерой или иным внешним устройством.

2.5. Если законом на Оператора будут возложены дополнительные обязанности (в том числе обязанности организатора распространения информации и требования Федерального закона от 07.07.2003 № 126-ФЗ и Федерального закона от 06.07.2016 № 374-ФЗ в применимом объёме), Оператор исполняет их в установленном порядке и в предусмотренном объёме. Исполнение таких обязанностей не раскрывает Пользователю сведения, разглашение которых запрещено законом, и не ограничивает право Пользователя на обжалование в порядке раздела A5.

2.6. Технические средства Сервиса используют сторонние криптографические библиотеки с открытым исходным кодом (протокол Olm). Оператор **не является разработчиком** этих библиотек и не гарантирует отсутствие в них уязвимостей; Оператор обеспечивает своевременное обновление используемых версий.

А3. Порядок использования Сервиса

3.1. **Допуск.** Сервис доступен Пользователю, зарегистрированному в Экосистеме Gramaton и акцептовавшему Пользовательское соглашение, Политику обработки ПД и «Соглашение о кибербезопасности». Использование Сервиса требует достижения 18 лет и необходимой дееспособности.

3.2. **Защищённый вход.** Доступ к разделу «Закрытые чаты» защищён PIN-кодом (строго 8 цифр): код задаётся при первом входе, проверяется вводом в поле поиска, хранится в виде необратимого значения (соль + хеш) в защищённом хранилище устройства, **не передаётся на сервер** и не выводится в логи и диагностику. Раздел автоматически блокируется при выходе с экрана и при уходе приложения в фон.

3.3. **Защита от перебора PIN.** После 3 неверных вводов подряд включается возрастающая пауза; после 5 неверных вводов подряд раздел **самоуничтожается** — удаляются список закрытых контактов, PIN-хеш и локальный кеш защищённых чатов. Переписка не шифруется PIN-кодом; самоуничтожение затрагивает локальные данные раздела.

3.4. **Устройства и ключи.** Новое Устройство регистрируется в Сервисе как **неодобренное** и не получает собственных копий сообщений, пока владелец не подтвердит его с другого уже одобренного Устройства. Число активных Устройств ограничивается настройками Сервиса (граница указывается Пользователю в интерфейсе). Устройство может быть отключено Пользователем; предусмотрена функция «выйти на всех устройствах». Переписка, отправленная до одобрения Устройства, ему **не передаётся**.

3.5. **Обязанности Пользователя:** сохранять конфиденциальность пароля, PIN-кода и кодов доступа; не передавать Устройство и коды третьим лицам; незамедлительно сообщать Оператору о подозрении на несанкционированный доступ (Пользовательское соглашение, п. 4.4); использовать Сервис в соответствии с назначением и законодательством РФ.

3.6. **Запрещается:** использовать Сервис для распространения информации, запрещённой законодательством РФ (экстремистские материалы, материалы с признаками порнографии, в том числе с участием несовершеннолетних, сведения о наркотических средствах, клевета и оскорбления, реклама запрещённых товаров и услуг, информация мошеннического характера); нарушать права третьих лиц, включая права интеллектуальной собственности; получать доступ к чужим аккаунтам; совершать действия, направленные на нарушение работы Сервиса и его защитных механизмов; использовать Сервис для массовых рассылок, не согласованных с получателями.

3.7. **Скриншоты и копирование.** Средствами операционной системы экран защищённых чатов блокируется от снятия скриншотов и записи экрана (насколько это позволяет платформа). Пользователю сообщается прямо: такая защита **не препятствует** съёмке экрана другим устройством (камерой) и не запрещает получателю офлайн-копирование в обход клиента, если он располагает достаточными средствами. Указанная защита — защита от обычных пользователей, а не средство абсолютной защиты контента.

3.8. **Ограничение, приостановление и прекращение доступа** применяются исключительно по закрытому перечню оснований (Пользовательское соглашение, п. 4.5): нарушение Соглашения или любого Приложения; размещение запрещённого Контента; предписание уполномоченного государственного органа; неиспользование учётной записи более 12 месяцев подряд. При ограничении доступа к Сервису Оператор: 3.8.1. направляет **мотивированное уведомление** с указанием основания, даты, срока действия и порядка обжалования — не позднее 3 (трёх) календарных дней до введения ограничения, а в случаях, требующих немедленного реагирования (угрозы безопасности, противоправные действия), — не позднее 1 (одного) рабочего дня с момента введения (ст. 13 Федерального закона от 31.07.2025 № 289-ФЗ); 3.8.2. сохраняет Пользователю доступ к Личному кабинету, договорам и их редакциям, истории операций и разделу жалоб (ч. 4 ст. 13 указанного Закона); 3.8.3. ограничивает доступ на **срочной** основе с автоматическим пересмотром; бессрочное ограничение не применяется; 3.8.4. обеспечивает право на досудебное обжалование в порядке раздела А5.

3.9. **Изменение условий.** Изменения в настоящее Приложение вносятся в порядке ст. 12 Федерального закона от 31.07.2025 № 289-ФЗ: уведомление не позднее чем за 45 (сорок пять) календарных дней — для изменений, затрагивающих тарифы, ответственность Сторон и порядок досудебного обжалования; не позднее чем за 15 (пятнадцать) календарных дней — для прочих изменений. Утратившие силу редакции хранятся и доступны Пользователю в Личном кабинете не менее 3 (трёх) лет с даты замены (ч. 5 ст. 5 указанного Закона).

А4. Расчёты, вознаграждение, возвраты

4.1. Использование базового функционала Сервиса является бесплатным, если иное прямо не установлено (Пользовательское соглашение, п. 7.1). Отдельные функции Сервиса могут предоставляться на платной основе — по подписке (Пользовательское соглашение, п. 7.2).

4.2. Платные функции Сервиса, если они предоставляются Пользователю, подключаются через функционал расчётов Экосистемы; списание производится с баланса Пользователя, учёт которого ведётся в соответствии с Приложением о сервисе «Кошелёк». Расчёты с Пользователями осуществляются через номинальный счёт Оператора в банке-партнёре (ст. 860.1 Гражданского кодекса РФ; Пользовательское соглашение, п. 7.3–7.5). 4.2.1. Отдельные функции Сервиса — защищённый раздел «Закрытые чаты» с обязательным сквозным шифрованием и защита исходящего контента от копирования — могут предоставляться при наличии у Пользователя активной подписки. При отсутствии подписки доступ к таким функциям не предоставляется: Пользователю отображается предложение о подключении с указанием состава функций и срока. Отключение подписки (отказ от автопродления, истечение срока) не влечёт удаления переписки и данных Пользователя — отключаются только соответствующие функции; переписка в закрытых чатах автоматически не расшифровывается и не становится доступной иным лицам.

4.3. Конкретные размеры платы за платные функции Сервиса, порядок списания, продления и возврата в настоящем Приложении **не устанавливаются**; они определяются соответствующим документом Оператора (оферта или Приложение по платёжной функции) и отображаются Пользователю до подтверждения оплаты. Сведения о факте оплаты, сроке и результате списания обрабатываются в целях исполнения договора и отчётности (Часть В, разделы В4–В6).

4.4. При отказе Пользователя от платной функции (отмена автопродления) доступ к оплаченному периоду сохраняется; данные Пользователя при этом **не удаляются** — отключается только функциональность, требующая подписки. Возвраты производятся в порядке, установленном соответствующим документом Оператора о расчётах, и в соответствии с законодательством о защите прав потребителей (в применимой части).

4.5. Чеки формируются в соответствии с Федеральным законом от 22.05.2003 № 54-ФЗ в случаях, когда Оператор обязан их формировать. Оператор не является налоговым агентом Пользователя — физического лица по операциям, не связанным с выплатой дохода.

А5. Споры и досудебный порядок

5.1. Пользователь вправе обратиться к Оператору через раздел «Жалобы» в Личном кабинете, интерфейс Сервиса или по адресу электронной почты Оператора. Жалоба должна содержать данные заявителя, идентификатор чата/сообщения/решения, суть нарушения со ссылкой на норму или пункт документа, обстоятельства и требование заявителя.

5.2. Обращения, связанные с применением мер Оператора в Сервисе (ограничение доступа к Сервису, удаление Контента, отказ в предоставлении функции), рассматриваются в порядке раздела 15 Пользовательского соглашения: регистрация жалобы — не позднее 1 (одного) рабочего дня; **срок рассмотрения — не более 15 (пятнадцати) календарных дней** со дня регистрации (ч. 2 ст. 14 Федерального закона от 31.07.2025 № 289-ФЗ); при признании жалобы обоснованной применённая мера отменяется в течение **48 (сорока восьми) часов**. Решение оформляется мотивированно и направляется заявителю (ч. 3 ст. 13, ст. 14 указанного Закона).

5.3. На время рассмотрения жалобы исполнение обжалуемой меры в части, не связанной с удержанием средств, может быть приостановлено. Рассмотрение осуществляется лицом (подразделением), не участвовавшим в принятии обжалуемого решения.

5.4. Отказ в удовлетворении жалобы не лишает Пользователя права обратиться в суд. До обращения в суд обязателен претензионный порядок: письменная претензия, срок ответа — 30 (тридцать) календарных дней (Пользовательское соглашение, п. 9.3).

5.5. По вопросам обработки персональных данных Пользователь вправе обратиться в порядке раздела B9 настоящего Приложения и главы 3 Федерального закона № 152-ФЗ, а также в Роскомнадзор и в суд.

A6. Ответственность и ограничения

6.1. Сервис предоставляется «как есть» (as is). Оператор не гарантирует бесперебойную и безошибочную работу программного обеспечения (Пользовательское соглашение, п. 8.1), принимая при этом разумные меры для её поддержания.

6.2. Оператор не отвечает за: действия других Пользователей; содержание передаваемых сообщений; последствия компрометации устройства Пользователя (вредоносное программное обеспечение, перехват экрана, кейлоггеры); разглашение Пользователем собственных пароля, PIN-кода и кодов доступа; утрату Пользователем доступа к устройству; обстоятельства непреодолимой силы.

6.3. Пределы ответственности Оператора определяются Пользовательским соглашением (п. 8.3) и не применяются в части, в которой ограничение ответственности не допускается законом (в том числе права потребителя по Закону РФ от 07.02.1992 № 2300-1 и ответственность за вред жизни и здоровью).

6.4. **Честные ограничения защиты (раскрываются Пользователю до начала использования).** 6.4.1. Если у собеседника нет ни одного Устройства с зарегистрированными ключами, сообщение отправляется **без сквозного шифрования** с явной пометкой «не зашифровано» в интерфейсе. Ложная индикация защиты не применяется: замок отображается только тогда, когда шифрование фактически применено. 6.4.2. E2EE защищает канал передачи, но **не защищает** от: Устройства, подключённого и одобренного владельцем аккаунта; заражённого или физически доступного третьим лицам Устройства; социальной инженерии; снятия экрана внешней камерой. 6.4.3. Оператору доступны **метаданные** переписки (см. B2, B4): факт, время, участники и служебные характеристики передачи. Сквозное шифрование не скрывает метаданные. 6.4.4. Облачные резервные копии содержимого защищённой переписки Оператором не создаются; при этом Пользователю сообщается, что резервное копирование устройства средствами операционной системы (например, резервная копия приложения) может привести к сохранению расшифрованных данных в контуре, контролируемом Пользователем или производителем платформы, и Оператор за это не отвечает.

ЧАСТЬ B. ОСОБЕННОСТИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

B1. Правовые основания обработки

- **п. 1 ч. 1 ст. 6 152-ФЗ** — согласие субъекта персональных данных (регистрация в Экосистеме, акцепт Соглашения и Политики, отдельные согласия на функции Сервиса).
- **п. 5 ч. 1 ст. 6 152-ФЗ** — исполнение договора, стороной которого является субъект (Пользовательское соглашение и настоящее Приложение): предоставление доступа, доставка сообщений, работа механизмов защиты, рассмотрение обращений.
- **п. 2 ч. 1 ст. 6 152-ФЗ** — исполнение обязанностей, возложенных на Оператора законом: 152-ФЗ (ст. 18.1, 19 — обеспечение безопасности, внутренний контроль, аудит), 149-ФЗ (модерация и ограничение доступа к запрещённой информации), 126-ФЗ/374-ФЗ (в применимом к Оператору объёме), 289-ФЗ (ст. 13–14 — мотивированные решения и досудебное обжалование).
- **п. 4 ч. 1 ст. 6 152-ФЗ** — защита жизни, здоровья и иных жизненно важных интересов субъекта (в объёме, необходимом для реагирования на угрозы жизни и здоровью, о которых Оператору стало известно из обращений).
- Иные основания (договоры с обработчиками, поручение обработки) — в соответствии с ч. 3 ст. 6 152-ФЗ.

B2. Категории ПД

Обычные: идентификатор аккаунта; имя (отображаемое имя), ник (username); номер телефона (для не-друзей отображается в маскированном виде); адрес электронной почты (если указан субъектом); аватар; хеш пароля; публичный идентификатор; статус присутствия («в сети», «был(а)…»).

Специальные (ст. 10 152-ФЗ): в Сервисе **не обрабатываются**. Специальные категории, обрабатываемые в иных Сервисах Экосистемы (документы, удостоверяющие личность; данные медицинской книжки; адрес регистрации), в Сервисе «Защищённая связь» не используются.

Биометрические (ст. 11 152-ФЗ):не обрабатываются. Ранее загруженные изображения лица удалены; сбор селфи и распознавание лиц не используются (решение Оператора от 29.09.2026,). Локальная биометрическая разблокировка приложения (например, отпечаток или распознавание лица средствами операционной системы) выполняется **самим устройством**; биометрические шаблоны Оператору не передаются и Оператором не обрабатываются.

Иные данные: - **содержание переписки** — текст сообщений и вложения, передаваемые в чатах. В защищённой переписке содержание Оператору **недоступно** (хранится в виде непрозрачных конвертов и шифртекста вложений); в незащищённых чатах (п. 6.4.1) содержание может обрабатываться Оператором для доставки; - **ключевой материал** — публичные ключи Устройств, регистрационные ключи и одноразовые ключи (prekeys), непрозрачные конверты. Приватные ключи на сервер не передаются; - **метаданные коммуникаций** — участники, чат, дата и время сообщения, размер и тип вложения, признак шифрования, статусы доставки и прочтения, отчёты о невозможности расшифрования; - **данные об устройствах и сессиях** — идентификатор и платформа Устройства, дата регистрации и последней активности, статус одобрения и отзыва, IP-адрес, сведения о регионе/местоположении по IP, сведения о клиенте (user agent), срок действия сессии; - **локальные данные устройства** — PIN-код (в виде соли и хеша), список закрытых контактов, локальный кеш закрытых чатов — обрабатываются **на устройстве** Пользователя и Оператору не передаются; - **данные о контактах и социальных связях** — список контактов и статусы связей, блокировки; - **обращения и жалобы** — сведения о жалобах на контент и на Пользователей, материалы рассмотрения; - **сведения о подписке и расчётах** — план, срок действия, суммы, результат операции (без полных реквизитов банковской карты); - **технические журналы** — журналы событий безопасности и аудита Сервиса (без содержимого переписки и без ключей), факты согласий и версии принятых документов.

В3. Субъекты и источники данных

- **Субъекты:** Пользователи Сервиса (отправители и получатели сообщений); лица, обратившиеся к Оператору через формы обратной связи и жалобы.

- **Источники:** сам субъект (регистрация, настройки Сервиса, отправляемые сообщения, обращения); технические данные, формируемые при использовании Сервиса (устройства, сессии, метаданные коммуникаций, журналы); Оператор — в части учётных данных, сформированных при регистрации в Экосистеме.
- Специальные категории ПД и сведения о третьих лицах из иных Сервисов Экосистемы в Сервисе не используются.

B4. Цели обработки (цель → данные → основание)

Цель	Состав данных	Основание
Регистрация, ведение и защита учётной записи, доступ к Сервису	идентификатор, имя, ник, телефон (маска), e-mail (если указан), аватар, хеш пароля	ст. 6 ч. 1 п. 1, п. 5
Обмен сообщениями и доставка конвертов, синхронизация между Устройствами одного Пользователя	содержание (в защищённом виде), метаданные коммуникаций, статусы доставки/прочтения	ст. 6 ч. 1 п. 5
Обеспечение сквозного шифрования (E2EE)	публичные ключи Устройств, регистрационные и одноразовые ключи, непрозрачные конверты	ст. 6 ч. 1 п. 5, п. 1
Защита от клонирования аккаунта и несанкционированного доступа (подтверждение и отзыв Устройств, «выйти на всех»)	данные об устройствах и сессиях, журнал событий устройств	ст. 6 ч. 1 п. 1, п. 5, п. 2 (152-ФЗ ст. 19)
Работа защищённого раздела «Закрытые чаты» (PIN, автоблокировка, самоуничтожение локальных данных)	локальные данные устройства (PIN-хеш, список контактов, локальный кеш) — обрабатываются на устройстве	ст. 6 ч. 1 п. 5
Защита исходящего контента от копирования и снятия экрана	признак «защищено» у сообщения; сведения о подписке	ст. 6 ч. 1 п. 5
Обеспечение безопасности, предотвращение мошенничества и нарушений, разбор инцидентов	журналы безопасности, метаданные коммуникаций, сведения об устройствах и сессиях	ст. 6 ч. 1 п. 2, п. 5

Цель	Состав данных	Основание
Модерация Контента и исполнение законных требований уполномоченных органов	сведения о жалобах и обращениях, метаданные коммуникаций, содержание — в объёме, к которому у Оператора есть законный доступ	ст. 6 ч. 1 п. 2 (149-ФЗ, 126-ФЗ/ 374-ФЗ в применимом объёме)
Рассмотрение обращений, претензий и досудебных жалоб	данные обращения, материалы переписки, представленные сторонами	ст. 6 ч. 1 п. 2 (289-ФЗ), п. 5
Расчёты по платным функциям Сервиса и отчётность	сведения о подписке, суммы и результаты операций	ст. 6 ч. 1 п. 5; п. 2 (налоговое законодательство, 54-ФЗ)
Подтверждение правомерности обработки (согласия, версии документов)	факты согласий, версии и даты акцепта документов	ст. 6 ч. 1 п. 2

B5. Сроки обработки и хранения

Данные	Срок	Основание	По истечении
Учётные данные, необходимые для исполнения договора	срок использования Сервиса + 3 (три) года после удаления учётной записи	Политика (раздел 6), договор	уничтожение или обезличивание
Содержание переписки	не более 6 (шести) месяцев с момента отправки, если Пользователь не установил более короткий срок (автоудаление) и не удалил чат ранее	Политика (раздел 6.2); настройки Сервиса (ст. 5 152-ФЗ — минимизация)	удаление
Метаданные коммуникаций, логи и метаданные Сервиса	1 (один) год	Политика (раздел 6.2)	уничтожение или обезличивание
	1 (один) год		

Данные	Срок	Основание	По истечении
Данные о фактах передачи сообщений (служебные сведения о передаче)		Политика (раздел 6.2); 126-ФЗ/374-ФЗ в применимом объёме	уничтожение
Данные об устройствах, сессиях и журнал событий безопасности	срок действия сессии и далее — 1 (один) год	Политика (раздел 6.2); 152-ФЗ ст. 19	уничтожение или обезличивание
Ключевой материал (публичные ключи, prekeys, конверты)	до отзыва Устройства или удаления учётной записи; использованные одноразовые ключи — до истечения срока хранения соответствующей переписки	договор; минимизация	удаление
Обращения, жалобы и материалы споров	3 (три) года	289-ФЗ; договор	уничтожение
Сведения о подписке и расчётах	5 (пять) лет	налоговое законодательство	архив/уничтожение
Факты согласий и версии принятых документов	срок обработки + 3 (три) года	152-ФЗ (подтверждение правомерности)	уничтожение
Локальные данные устройства (PIN-хеш, список закрытых контактов, локальный кеш)	до удаления Пользователем или самоуничтожения раздела	обработка на устройстве	удаление на устройстве

В6. Получатели и поручение обработки

- **Банк-партнёр** — расчёты по платным функциям (номинальный счёт); банк обрабатывает платёжные данные как самостоятельный оператор в рамках своей лицензии. Полные реквизиты банковских карт Оператором не обрабатываются.

- **Обработчики по поручению (ч. 3 ст. 6 152-ФЗ)** — лица, привлекаемые для обеспечения функционирования Сервиса (инфраструктура/ЦОД на территории РФ, техническая поддержка, рассылки служебных уведомлений) — на основании договоров с обязательствами конфиденциальности и требованиями к защите персональных данных. Перечень обработчиков ведётся Оператором.
- **Государственные органы** (в том числе Роскомнадзор, МВД, ФСБ, суды) — по мотивированным запросам в случаях, предусмотренных законом, в объёме, доступном Оператору. Оператор раскрывает сведения о переписке только в предусмотренных законом случаях и в предусмотренном объёме, фиксируя факт раскрытия.
- **Иные Пользователи** — получатели сообщений получают переданные им данные (в защищённом виде), а также сведения профиля в объёме, определяемом настройками Пользователя.
- Поручение обработки третьим лицам не даёт им права использовать персональные данные в собственных целях.

B7. Трансграничная передача

7.1. Персональные данные, обрабатываемые в Сервисе, **хранятся на территории Российской Федерации** (ч. 5 ст. 18 152-ФЗ; Политика, раздел 6.1). Базы данных, содержащие персональные данные граждан РФ, размещены в РФ.

7.2. Передача персональных данных на территорию иностранных государств в рамках Сервиса **не осуществляется** (Политика, раздел 5.3). Если в отношении отдельных функций такая передача потребуется, она будет осуществляться исключительно на условиях ст. 12 152-ФЗ — с уведомлением уполномоченного органа и, при необходимости, с получением отдельного согласия субъекта, оформленного в соответствии с Политикой и Согласием на трансграничную передачу персональных данных (Пользовательское соглашение, п. 1.9.1).

7.3. Обработка персональных данных в Сервисе не преследует самостоятельных целей трансграничной передачи; сведения о резервном копировании и размещении — в разделе B8.

В8. Меры защиты

8.1. Организационные (152-ФЗ ст. 18.1, 19; ПП РФ от 01.11.2012 № 1119): - ответственный за организацию обработки персональных данных; ответственный за обеспечение безопасности ПД в ИСПДн; - перечень ИСПДн и отнесение системы ко **2-му уровню защищённости (УЗ-2)** (ПП-1119); - модель угроз и модель нарушителя; оценка вреда субъектам ПД; регламент реагирования на инциденты; план восстановления; - правила доступа (роли, принцип минимальных привилегий, маскирование ПД, основание для раскрытия), журнал доступа, ознакомление работников; - внутренний контроль соответствия обработки, ведение реестра мер и реестра обработчиков.

8.2. Технические (Приказ ФСТЭК России от 18.02.2013 № 21, базовый набор мер для УЗ-2): - идентификация и аутентификация (пароли с хешированием bcrypt, одноразовые коды — MFA, короткие сессии с криптоподписью); - управление доступом (RBAC), разграничение доступа к ПД, маскирование с фиксацией основания раскрытия; - регистрация событий безопасности: журнал аудита и журнал событий безопасности Сервиса (без содержимого переписки и без ключей); - защита канала: TLS через обратный прокси, HSTS/CSP, блокировка подозрительной активности, закрытые служебные порты, защита веб-периметра; - защита среды исполнения (изоляция сервисов в контейнерах, ограниченный набор ПО, обновление зависимостей); - резервное копирование с шифрованием копий и проверкой восстановления — на территории РФ; - привязка TLS-сертификата на клиенте (pinning) и защита учётных данных на устройстве (защищённое хранилище).

8.3. Криптографические: - сквозное шифрование переписки: протокол Olm (Double Ratchet, X3DH-подобный handshake) на базе библиотеки libolm (мобильный и веб-клиенты); серверная часть криптографии **не выполняет**; - шифрование вложений: AES-256-GCM на клиенте; ключ и вектор шифрования передаются только внутри зашифрованного конверта; на сервере хранится шифртекст (длина файла превышает исходную на размер тега аутентичности); - передача данных — по защищённому каналу (TLS; в web — WebCrypto, в мобильном — встроенные криптопровайдеры платформы); - применяемые криптографические средства **не являются сертифицированными СКЗИ**;

8.4. Контроль защищённости — периодические проверки защищённости веб-периметра, аудит конфигураций и прав доступа, анализ уязвимостей зависимостей; результаты фиксируются Оператором.

В9. Права субъекта ПД

9.1. Пользователь (субъект персональных данных) имеет права, предусмотренные главой 3 Федерального закона № 152-ФЗ: на получение информации об обработке своих персональных данных; на доступ к ним; на уточнение (обновление, изменение); на блокирование или уничтожение, если они являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели; на отзыв согласия; на обжалование действий (бездействия) Оператора в уполномоченный орган по защите прав субъектов персональных данных (Роскомнадзор) или в суд.

9.2. Порядок обращения: через форму обратной связи в приложении/Сервисе либо по адресу электронной почты **help@gramaton.pro** (официальный адрес Оператора: ustin@gramaton.pro). Запрос должен содержать сведения, позволяющие идентифицировать субъекта (имя и номер телефона, привязанный к учётной записи), и суть требования.

9.3. Срок рассмотрения обращения — **30 (тридцать) дней** с момента получения, если законом не установлен меньший срок. Ответ направляется в форме, позволяющей подтвердить его получение.

9.4. Отзыв согласия не затрагивает обработку персональных данных, правовым основанием которой является не согласие, а исполнение договора или исполнение обязанностей, возложенных на Оператора законом, а также сведения, обязательные к хранению в силу закона.

9.5. Удаление учётной записи влечёт удаление локальных данных на устройстве и прекращение обработки соответствующих данных Оператором, за исключением данных, хранение которых обязательно по закону.

B10. Специфика Сервиса

10.1. **Тайна связи и переписки.** Оператор обеспечивает конфиденциальность коммуникаций: сведения о переписке и её содержании не раскрываются третьим лицам, кроме случаев, прямо предусмотренных законом. Сквозное шифрование делает содержание защищённой переписки технически недоступным для Оператора: в серверной части хранятся непрозрачные конверты, а также метаданные коммуникаций (см. B2, B4).

10.2. **Особый режим «Закрытых чатов».** Для этих чатов шифрование применяется обязательно: при отсутствии доступных ключей сообщение не отправляется открытым текстом — Пользователь уведомляется о невозможности защищённой отправки. Переписка закрытых чатов скрыта из общего списка чатов и поиска; локальный кеш раздела и ключи шифрования хранятся на устройстве в защищённом виде; предусмотрены автоблокировка, возрастающая пауза при переборе PIN и самоуничтожение локальных данных раздела после исчерпания попыток (см. A3.3).

10.3. **Уведомления.** Уведомления о новых сообщениях в закрытых чатах формируются без текста сообщения, чтобы содержание не отображалось на заблокированном экране устройства.

10.4. **Автоудаление.** Пользователь может установить автоудаление сообщений в чате; по достижении срока сообщения удаляются из Сервиса. Автоудаление является реализацией принципа минимизации (ч. 5 ст. 5 152-ФЗ) и не отменяет обязанностей Оператора по хранению сведений, которые он обязан хранить по закону (см. B5).

10.5. **UGC и информационный посредник.** Содержание сообщений создаётся Пользователями. Оператор является информационным посредником (ст. 1253.1 ГК РФ), не проверяет содержание переписки в режиме реального времени и рассматривает жалобы на Контент в порядке, установленном Пользовательским соглашением (раздел 6) и разделом A5 настоящего Приложения. При наличии законного требования уполномоченного органа Оператор принимает предусмотренные законом меры (в том числе ограничение доступа к Контенту).

10.6. **Биометрия.** Биометрические персональные данные в Сервисе **не обрабатываются**. Локальная биометрическая разблокировка приложения (при её включении Пользователем) выполняется средствами операционной системы устройства; биометрические шаблоны не передаются Оператору и не хранятся в Сервисе.

10.7. **Несовершеннолетние.** Использование Сервиса предполагает достижение Пользователем 18 лет; Пользователь несёт ответственность за передачу своих устройств и данных третьим лицам.

10.8. **Геолокация.** Сервис не отслеживает местоположение Пользователя. Оператор может получать сведения о регионе/местоположении, определяемые по IP-адресу, — в целях безопасности и предотвращения мошенничества (B4).

10.9. **Ограничения защиты (раскрываются прямо).** E2EE защищает канал передачи данных, но не защищает от: Устройства, подключённого и одобренного владельцем аккаунта; заражённого Устройства; социальной инженерии; снятия экрана внешней камерой; работы средствами обхода режима защиты в случае, если устройство предоставлено третьему лицу. Оператору доступны метаданные коммуникаций.

Сводная таблица «данные × цель × основание × срок × получатель»

Данные	Цель	Основание	Срок	Получатель
Идентификатор аккаунта, имя, ник, телефон (маска), e-mail, аватар, хеш пароля	регистрация, идентификация, доступ к Сервису	ст. 6 ч. 1 п. 1, 5	использование + 3 года	обработчики (поддержка, инфраструктура в РФ)
Содержание переписки (текст, вложения)	обмен сообщениями	ст. 6 ч. 1 п. 5	не более 6 месяцев (или короче по настройке/удалению)	получатель сообщения; Оператору недоступно при E2EE
Публичные ключи устройств, регистрационные и одноразовые	обеспечение E2EE	ст. 6 ч. 1 п. 5, 1	до отзыва устройства / удаления УЗ	адресаты (через сер-

Данные	Цель	Основание	Срок	Получатель
ключи, непрозрачные конверты				вер), не Оператору
Метаданные коммуникаций (участники, время, размер, статусы доставки/прочтения, признак шифрования)	доставка сообщений, безопасность, разбор инцидентов	ст. 6 ч. 1 п. 5; п. 2	1 год	госорганы (по закону)
Сведения о фактах передачи сообщений (служебные)	исполнение требований законодательства	ст. 6 ч. 1 п. 2 (126-ФЗ/374-ФЗ в применимом объёме)	1 год	госорганы (по закону)
Данные об устройствах и сессиях (device_id, платформа, IP, регион, клиент, сроки)	защита от клонирования аккаунта, управление доступом, антифрод	ст. 6 ч. 1 п. 1, 5; п. 2 (152-ФЗ ст. 19)	срок сессии + 1 год	—
Журналы безопасности и аудита Сервиса (без контента и ключей)	контроль защищённости, доказуемость, ответы регулятору	ст. 6 ч. 1 п. 2 (152-ФЗ ст. 18.1, 19), п. 5	не менее 3 лет	госорганы (по закону)
Локальные данные устройства (PIN-хеш, список закрытых контактов, локальный кеш)	работа защищённого раздела «Закрытые чаты»	ст. 6 ч. 1 п. 5	до удаления/самоуничтожения на устройстве	не передаются Оператору
Контакты, связи, блокировки	работа Сервиса, ограничение нежелательных коммуникаций	ст. 6 ч. 1 п. 5	до удаления УЗ	—
Обращения, жалобы, материалы споров	модерация, рассмотрение споров и обжалований	ст. 6 ч. 1 п. 2 (149-ФЗ, 289-ФЗ), п. 5	3 года	—

Данные	Цель	Основание	Срок	Получатель
Сведения о подписке и расчётах (план, срок, суммы, результат)	расчёты за платные функции, отчётность	ст. 6 ч. 1 п. 5; п. 2 (налоговое, 54-ФЗ)	5 лет	банк-партнёр, ФНС
Уведомления и служебные сообщения Сервиса	информирование о событиях аккаунта и безопасности	ст. 6 ч. 1 п. 5	до прочтения/удаления, далее по общим срокам	—
Факты согласий, версии принятых документов	подтверждение правомерности обработки	ст. 6 ч. 1 п. 2	обработка + 3 года	—
Специальные категории (ст. 10)	—	**в Сервисе не обрабатываются**	—	—
Биометрические ПД (ст. 11)	—	**не обрабатываются** (локальная разблокировка — на устройстве)	—	—