



ПРАВИЛА ДОПУСТИМОГО ИСПОЛЬЗОВАНИЯ

(Acceptable Use Policy)

Платформа «Реккора» — reccora.ru

Редакция от «12» июля 2026 г.

Дата вступления в силу: «12» июля 2026 г.

1. Общие положения

1.1. Настоящие Правила допустимого использования (далее — «Правила») устанавливают обязательные требования к порядку использования платформы «Реккора» (далее — «Платформа»), доступной по адресу reccora.ru и через иные каналы доступа (в том числе Telegram-бот).

1.2. Настоящие Правила являются неотъемлемой частью Пользовательского соглашения (reccora.ru/terms) и Договора-оферты на оказание платных услуг (reccora.ru/offer). Регистрация на Платформе и/или использование её функциональности означает согласие с настоящими Правилами.

1.3. Правила распространяются на всех Пользователей Платформы, включая пользователей бесплатного тарифа, платных подписчиков, участников командных аккаунтов и пользователей Telegram-бота.

1.4. Правообладатель Платформы — Общество с ограниченной ответственностью «РЕККОРА» (ОГРН: 1267700232568, ИНН: 9734027193), далее — «Правообладатель».

1.5. Правообладатель вправе вносить изменения в настоящие Правила в одностороннем порядке, уведомив Пользователей путём размещения новой редакции на Платформе. Актуальная версия доступна по адресу reccora.ru/acceptable-use.

1.6. Незнание настоящих Правил не освобождает Пользователя от ответственности за их нарушение.

2. Назначение Платформы и допустимое использование

2.1. Платформа «Реккора» предназначена исключительно для:

- а) загрузки бизнес-данных из файлов (Excel, CSV, 1С-выгрузки, CRM-экспорт) с целью автоматического анализа, прогнозирования и визуализации;
- б) использования AI-аналитики по направлениям: продажи, маркетинг, финансы, операции;
- в) построения прогнозов на основе исторических данных;
- г) создания интерактивных лайвбордов (визуализаций);
- д) взаимодействия с AI-диалогом для уточнения параметров анализа;
- е) экспорта отчётов и визуализаций;
- ж) получения консультаций от универсального AI-ассистента по бизнес-вопросам.

2.2. Пользователь обязуется использовать Платформу исключительно в законных целях, в соответствии с её функциональным назначением и настоящими Правилами.

2.3. Примеры допустимого использования:

- анализ данных о продажах собственного бизнеса;
- прогнозирование выручки, расходов, cash-flow;

- построение визуализаций для внутренних отчётов и презентаций;
- ABC/XYZ-анализ товарного ассортимента;
- RFM-анализ клиентской базы;
- план-факт анализ бюджета;
- анализ эффективности маркетинговых каналов;
- использование AI-ассистента для генерации бизнес-идей и текстов.

3. Ограничения по загружаемым данным

3.1. Запрещённые категории данных

Пользователю запрещается загружать на Платформу следующие данные:

3.1.1. Данные, составляющие государственную тайну:

- сведения, отнесённые к государственной тайне в соответствии с Законом РФ от 21.07.1993 № 5485-1 «О государственной тайне»;
- документы с грифами «Особой важности», «Совершенно секретно», «Секретно»;
- любые сведения из перечня, утверждённого Указом Президента РФ от 30.11.1995 № 1203.

3.1.2. Персональные данные специальных категорий (статья 10 152-ФЗ):

- данные о расовой и национальной принадлежности;
- данные о политических взглядах;
- данные о религиозных или философских убеждениях;
- данные о состоянии здоровья;
- данные об интимной жизни;
- данные о судимостях.

Исключение: загрузка допускается при наличии у Пользователя законного основания для обработки таких данных (пункты 2–10 части 2 статьи 10 152-ФЗ) и под полную ответственность Пользователя.

3.1.3. Биометрические персональные данные (статья 11 152-ФЗ):

- фотографии, используемые для идентификации;
- отпечатки пальцев, образцы голоса, результаты ДНК-тестов;
- иные биологические характеристики, используемые для идентификации.

3.1.4. Данные, полученные незаконным путём:

- данные, добытые в результате неправомерного доступа к компьютерной информации (статья 272 УК РФ);
- данные, полученные в результате нарушения тайны переписки, телефонных переговоров, почтовых и иных сообщений (статья 138 УК РФ);
- данные, добытые путём мошенничества, кражи или иным преступным способом;
- данные, полученные с нарушением коммерческой тайны (статья 183 УК РФ).

3.1.5. Данные, нарушающие права третьих лиц:

- персональные данные третьих лиц, загруженные без законного основания для обработки;
- данные, составляющие коммерческую тайну третьих лиц, к которым Пользователь не имеет права доступа;
- данные, защищённые авторским правом, загруженные без разрешения правообладателя;
- данные, полученные с нарушением режима банковской тайны (статья 857 ГК РФ).

3.1.6. Данные, содержащие вредоносный код:

- файлы, содержащие вирусы, трояны, шпионское ПО, ransomware;
- файлы с эксплойтами и вредоносными макросами;
- файлы, намеренно повреждённые для эксплуатации уязвимостей парсеров.

3.1.7. Данные, связанные с противоправной деятельностью:

- данные, связанные с финансированием терроризма и экстремизма;
- данные, связанные с легализацией (отмыванием) доходов, полученных преступным путём;
- данные, связанные с оборотом наркотических средств и психотропных веществ;
- данные, связанные с торговлей людьми;
- данные, связанные с иной деятельностью, запрещённой законодательством РФ.

3.2. Ответственность за загружаемые данные

3.2.1. Пользователь несёт полную ответственность за содержание, законность и достоверность загружаемых данных.

3.2.2. Правообладатель не осуществляет предварительную модерацию (проверку) загружаемого контента, однако вправе удалить данные и заблокировать Аккаунт при обнаружении нарушений.

3.2.3. Если загруженные данные содержат персональные данные третьих лиц, Пользователь гарантирует наличие законного основания для их обработки и передачи на Платформу (часть 3 статьи 6 152-ФЗ).

3.2.4. Пользователь обязуется возместить Правообладателю все убытки (включая штрафы, судебные издержки, расходы на юридическую помощь), возникшие вследствие нарушения Пользователем требований настоящего раздела.

4. Запрещённые действия при использовании Платформы

4.1. Технические нарушения

Пользователю запрещается:

- а) предпринимать попытки несанкционированного доступа к серверной инфраструктуре, базам данных, программному коду Платформы или данным других Пользователей;
- б) осуществлять автоматизированный сбор данных (scraping, crawling, parsing) с Платформы с использованием ботов, скриптов, парсеров и иных автоматизированных средств;
- в) совершать действия, направленные на нарушение работоспособности Платформы, включая DDoS-атаки, флуд, массовую загрузку файлов с целью перегрузки серверов;
- г) эксплуатировать уязвимости Платформы (включая уязвимости AI-модулей, промпт-инъекции и иные техники обхода ограничений);
- д) модифицировать, декомпилировать, дизассемблировать или осуществлять обратную разработку (reverse engineering) программного обеспечения Платформы;
- е) извлекать исходный код, алгоритмы, модели, веса AI-модулей или иную интеллектуальную собственность Правообладателя;
- ж) обходить технические средства защиты, системы аутентификации, ограничения доступа, лимиты тарифных планов;
- з) использовать VPN, прокси или иные средства для сокрытия реального IP-адреса с целью обхода блокировок;
- и) генерировать искусственную нагрузку на API Платформы;
- к) подключаться к Платформе через неофициальные клиенты, API-обёртки или интеграции без согласия Правообладателя.

4.2. Нарушения правил учётных записей

Пользователю запрещается:

- а) создавать более одного Аккаунта (множественные аккаунты);
- б) использовать одноразовые (временные) адреса электронной почты для регистрации;
- в) регистрировать Аккаунт на вымышленные или чужие данные;
- г) передавать данные для доступа к Аккаунту третьим лицам (за исключением командного функционала, если он предусмотрен выбранным тарифом);
- д) продавать, сдавать в аренду, передавать за вознаграждение доступ к Аккаунту или подписке;
- е) использовать чужой Аккаунт;
- ж) создавать аккаунты-«пустышки» для использования бесплатных лимитов (abuse of free tier).

4.3. Коммерческие нарушения

Пользователю запрещается:

- а) использовать Платформу для создания конкурирующих продуктов или сервисов (в том числе путём анализа функциональности, алгоритмов, интерфейса);
- б) перепродавать результаты работы Платформы как собственный сервис (white-label, reselling) без письменного согласия Правообладателя;
- в) использовать товарный знак, наименование, логотип «Реккора» / «Reccora» в коммерческих целях без письменного согласия;
- г) копировать, воспроизводить, распространять дизайн, тексты, графические элементы Платформы;
- д) создавать производные продукты на основе программного обеспечения Платформы.

4.4. Злоупотребление AI-функциональностью

Пользователю запрещается:

- а) использовать AI-диалог и AI-ассистент для генерации контента, нарушающего законодательство РФ (экстремистские материалы, призывы к насилию, клевета, порнография, пропаганда наркотиков);
- б) использовать AI-модули для генерации заведомо ложной финансовой отчётности, фальсифицированных данных, поддельных документов;
- в) применять техники промпт-инъекций (prompt injection) для обхода ограничений AI-модулей или получения несанкционированного доступа к системным промптам;
- г) целенаправленно провоцировать AI-модули на генерацию вредоносного, незаконного или неэтичного контента;
- д) использовать результаты работы AI для введения третьих лиц в заблуждение, выдавая автоматически сгенерированные результаты за результаты профессионального аудита, экспертизы или консультации;
- е) массово генерировать запросы к AI-модулям с целью исчерпания лимитов, перегрузки системы или извлечения системных промптов.

4.5. Нарушения при командном использовании

При использовании командного функционала (если он предусмотрен тарифом) дополнительно запрещается:

- а) приглашать в команду лиц, не являющихся сотрудниками или подрядчиками организации Пользователя;
- б) превышать максимальное количество пользователей, предусмотренное тарифом;
- в) использовать командные аккаунты для предоставления доступа к Платформе в коммерческих целях (reselling);
- г) назначать роли, не соответствующие реальным полномочиям участника (например, предоставлять роль «Наблюдатель» лицу, которое фактически ведёт анализ, с целью обхода лимитов).

5. Правила использования Telegram-бота

5.1. При использовании Telegram-бота Платформы Пользователь обязан соблюдать настоящие Правила в полном объеме, а также правила сервиса Telegram (Terms of Service).

5.2. Дополнительно запрещается:

- а) использовать Telegram-бот для массовой рассылки сообщений (spam);
- б) автоматизировать взаимодействие с ботом через сторонние скрипты и Telegram API без согласия Правообладателя;
- в) передавать ссылку на бот третьим лицам для использования от имени Аккаунта Пользователя;
- г) загружать через бот файлы, нарушающие требования раздела 3 настоящих Правил.

5.3. Все ограничения тарифного плана (лимиты запросов, доступные модули) применяются к использованию Telegram-бота в полном объеме.

6. Технические лимиты и добросовестное использование (Fair Use)

6.1. Платформа устанавливает технические лимиты для обеспечения стабильности и качества обслуживания всех Пользователей:

Параметр	Ограничение
Максимальный размер загружаемого файла	Определяется Тарифным планом (см. reccora.ru/pricing)
Максимальное количество строк в файле	Определяется Тарифным планом
Количество запросов к AI-модулям	Определяется Тарифным планом
Частота запросов (rate limit)	Не более 10 запросов в минуту
Объем хранимых данных (на Аккаунт)	Определяется Тарифным планом
Количество одновременных загрузок	Не более 3 файлов одновременно
Максимальная длина сообщения в AI-диалоге	2 000 символов

6.2. Правообладатель вправе изменять технические лимиты для обеспечения стабильности Платформы, уведомив Пользователей через интерфейс Платформы.

6.3. Политика добросовестного использования (Fair Use):

- а) Пользователь обязуется использовать Платформу добросовестно, не создавая чрезмерную нагрузку на инфраструктуру;
- б) при обнаружении аномально высокой нагрузки от конкретного Аккаунта (значительно превышающей средний уровень использования) Правообладатель вправе временно ограничить доступ и связаться с Пользователем для выяснения обстоятельств;
- в) систематическое превышение разумных объемов использования может служить основанием для перевода на более высокий Тарифный план или применения дополнительных ограничений.

7. Мониторинг и обнаружение нарушений

7.1. Правообладатель вправе осуществлять автоматизированный мониторинг использования Платформы для выявления нарушений настоящих Правил, включая:

- а) мониторинг частоты и объема запросов (для выявления DDoS, scraping, abuse);
- б) анализ паттернов использования (для выявления множественных аккаунтов, обхода лимитов);
- в) проверку загружаемых файлов на наличие вредоносного кода (антивирусное сканирование);
- г) журналирование действий в Аккаунте (логирование).

7.2. Правообладатель НЕ осуществляет:

- а) ручную проверку содержания загруженных бизнес-данных (если нет обоснованного подозрения на нарушение);
- б) чтение текста запросов Пользователя к AI-диалогу (если нет обоснованного подозрения на злоупотребление);
- в) передачу данных мониторинга третьим лицам (за исключением случаев, предусмотренных законодательством).

7.3. Пользователь вправе сообщить о нарушениях настоящих Правил другими Пользователями, направив обращение на abuse@reccora.ru.

8. Меры реагирования на нарушения

8.1. В случае нарушения настоящих Правил Правообладатель вправе применить следующие меры (в зависимости от характера и тяжести нарушения):

Мера	Описание	Когда применяется
Предупреждение	Уведомление по email о нарушении с требованием прекратить	Первичное незначительное нарушение
Ограничение функциональности	Временное снижение лимитов, отключение отдельных функций	Превышение лимитов, abuse of free tier
Временная блокировка	Приостановка доступа к Аккаунту на срок от 1 до 30 дней	Повторные нарушения, технические атаки
Удаление контента	Удаление загруженных файлов, нарушающих Правила	Запрещённые категории данных (раздел 3)
Постоянная блокировка	Безвозвратная блокировка Аккаунта, удаление данных	Грубые нарушения, угроза безопасности, повторные нарушения после предупреждений
Обращение в правоохранительные органы	Передача информации в компетентные органы РФ	Признаки уголовно наказуемого деяния

8.2. Грубыми нарушениями, влекущими немедленную постоянную блокировку без предварительного предупреждения, признаются:

- а) загрузка данных, составляющих государственную тайну;
- б) загрузка данных, связанных с финансированием терроризма или экстремизма;
- в) проведение DDoS-атак или иных кибератак на инфраструктуру Платформы;
- г) несанкционированный доступ к данным других Пользователей;
- д) распространение вредоносного программного обеспечения через Платформу;
- е) использование Платформы для легализации (отмывания) преступных доходов;
- ж) систематическое и умышленное создание множественных аккаунтов для обхода блокировок.

8.3. При временной или постоянной блокировке Пользователь уведомляется по электронной почте с указанием:

- а) факта и даты блокировки;
- б) основания блокировки (с указанием конкретного пункта настоящих Правил);
- в) срока блокировки (для временной);
- г) порядка обжалования.

8.4. Возврат денежных средств при блокировке за нарушение Правил не производится (пункт 9.2.6 Договора-оферты).

9. Порядок обжалования

9.1. Пользователь вправе обжаловать решение о блокировке Аккаунта или применении иных мер, направив мотивированное обращение на адрес arreal@reccora.ru в течение 30 (тридцати) календарных дней с момента получения уведомления о блокировке.

9.2. Обращение должно содержать:

- а) ФИО Пользователя (наименование организации);
- б) адрес электронной почты, привязанный к Аккаунту;
- в) дату блокировки;
- г) обоснование несогласия с решением;
- д) подтверждающие документы (при наличии).

9.3. Правообладатель рассматривает обращение в течение 15 (пятнадцати) рабочих дней и направляет Пользователю мотивированный ответ.

9.4. Решение Правообладателя по результатам рассмотрения обжалования является окончательным в рамках досудебного урегулирования. Пользователь вправе обратиться в суд в порядке, установленном Пользовательским соглашением.

10. Уведомление о нарушениях (отчёт о злоупотреблениях)

10.1. Любое лицо (в том числе не являющееся Пользователем) вправе сообщить о нарушении настоящих Правил, направив обращение на abuse@reccora.ru.

10.2. Обращение должно содержать:

- а) описание предполагаемого нарушения;
- б) данные, позволяющие идентифицировать нарушителя (при наличии);
- в) подтверждающие материалы (скриншоты, логи, документы);
- г) контактные данные заявителя.

10.3. Правообладатель рассматривает обращение в течение 10 (десяти) рабочих дней и принимает меры при подтверждении нарушения.

10.4. Правообладатель не раскрывает данные заявителя нарушителю, за исключением случаев, предусмотренных законодательством.

11. Ответственность Пользователя

11.1. Пользователь несёт полную ответственность за соблюдение настоящих Правил.

11.2. За нарушение настоящих Правил Пользователь может нести:

- а) гражданско-правовую ответственность — возмещение убытков Правообладателю и/или третьим лицам;
- б) административную ответственность — в соответствии с КоАП РФ (статьи 13.11, 13.12, 13.13, 13.14 и др.);
- в) уголовную ответственность — в соответствии с УК РФ (статьи 137, 138, 159, 165, 171, 183, 272, 273, 274 и др.).

11.3. Пользователь обязуется возместить Правообладателю все убытки, включая:

- а) реальный ущерб (расходы на устранение последствий нарушения, расходы на восстановление инфраструктуры);
- б) упущенную выгоду;
- в) штрафы, наложенные на Правообладателя государственными органами вследствие действий Пользователя;
- г) судебные издержки и расходы на юридическую помощь.

12. Программа ответственного раскрытия уязвимостей (Responsible Disclosure)

12.1. Если Пользователь обнаружил уязвимость в безопасности Платформы, Правообладатель просит сообщить о ней ответственно:

- а) направить описание уязвимости на security@reccora.ru;
- б) не эксплуатировать уязвимость;
- в) не раскрывать информацию о ней публично до устранения;
- г) не использовать уязвимость для доступа к данным других Пользователей.

12.2. Правообладатель обязуется:

- а) рассмотреть сообщение об уязвимости в течение 5 (пяти) рабочих дней;
- б) не применять меры ответственности к лицу, добросовестно сообщившему об уязвимости;
- в) уведомить заявителя об устранении уязвимости.

12.3. Программа ответственного раскрытия не распространяется на:

- а) целенаправленное тестирование на проникновение без согласия Правообладателя;
- б) социальную инженерию в отношении сотрудников Правообладателя;
- в) физическое проникновение на объекты Правообладателя;
- г) DDoS-атаки и иные действия, нарушающие работоспособность Платформы.

13. Заключительные положения

13.1. Настоящие Правила являются неотъемлемой частью Пользовательского соглашения (reccora.ru/terms) и Договора-оферты (reccora.ru/offer).

13.2. В случае противоречий между настоящими Правилами и Пользовательским соглашением приоритет имеют настоящие Правила в части вопросов, непосредственно касающихся допустимого использования.

13.3. Правообладатель вправе вносить изменения в настоящие Правила в одностороннем порядке. Новая редакция вступает в силу с момента размещения на Платформе.

13.4. Актуальная редакция настоящих Правил всегда доступна по адресу reccora.ru/acceptable-use.

13.5. Вопросы, не урегулированные настоящими Правилами, разрешаются в соответствии с Пользовательским соглашением и законодательством Российской Федерации.

13.6. К настоящим Правилам применяется законодательство Российской Федерации.

Контактные адреса:

Общие вопросы: info@reccora.ru

Сообщения о нарушениях: support@reccora.ru

Обжалование блокировок: support@reccora.ru

Уязвимости безопасности: support@reccora.ru

Персональные данные: support@reccora.ru

Реквизиты Правообладателя:

ООО «РЕККОРА»

ОГРН: 1267700232568

ИНН/КПП: 9734027193 / 773401001

Юридический адрес: 123308, г. Москва, вн. тер. г. муниципальный округ Хорошево-Мневники, Новохорошевский проезд, д. 7, помещение 6П

Веб-сайт: reccora.ru