Локально или в облако: что реально требует 152-ФЗ от B2B AI в 2026 году

Temadev

2026-05-14

Локально или в облако: что реально требует 152-ФЗ от B2B AI в 2026 году

Почему все вдруг стали бояться облака

30 мая 2025 года в России вступили в силу новые штрафы за утечки персональных данных. Размер санкций изменился радикально: утечка от 100 000 субъектов — до 20 млн ₽, повторное нарушение — оборотный штраф до 500 млн ₽. Параллельно, по данным Habr со ссылкой на статистику Роскомнадзора, за 2025 год возбуждено более 600 уголовных дел по статье 272.1 — неправомерный доступ к компьютерной информации.

Рынок отреагировал предсказуемо: консультанты, юристы и интеграторы массово стали советовать «делать всё on-prem». Это понятная реакция, но она некорректна как универсальное правило. Подавляющее большинство B2B AI-проектов — автоматизация спецтехники, производства, строительства, оптовой торговли — оперирует данными юридических лиц. ИНН, название компании, корпоративный email, должность ЛПР — это **не персональные данные** по смыслу 152-ФЗ. Закон защищает физических лиц, а не организации.

Задать правильный вопрос важно: не «облако или сервер?», а «что именно обрабатывает ваш AI и кому это принадлежит?»

Что 152-ФЗ защищает, а что нет

152-ФЗ «О персональных данных» распространяется на информацию, по которой можно идентифицировать **физическое лицо**. Из этого следует несколько практических следствий для B2B AI.

Зелёная зона — данные, с которыми AI-инструменты работают свободно без специального правового оформления: - Реквизиты юридических лиц: ИНН, ОГРН, название, адрес, корпоративный телефон, юридический email - Операционные данные без привязки к конкретному физлицу: парк техники, объёмы заявок, прайс-листы - Публичная информация: сайт клиента, опубликованные тендерные документы, прайсы - Обезличенные агрегаты: средняя скорость ответа, загруженность по дням недели, конверсия этапов воронки

Жёлтая зона — требует оформления, но облако не исключено: - Имена и телефоны контактных лиц (ЛПР) в компании-клиенте — технически это ПДн, но риск умеренный при наличии ДПО - Записи деловых переговоров и звонков —

требуют уведомления участников и договора об обработке - Формы с физическими адресами доставки (если это домашний адрес)

Красная зона — облако реально рискованно или прямо запрещено: - Биометрия: голосовые отпечатки, фотографии лиц → штрафы до 15–20 млн ₽ за утечку - Специальные категории ПДн: диагнозы, кредитные истории, данные о вероисповедании, данные о судимостях - Данные физических лиц (покупателей, пациентов, работников) без обезличивания - Любые данные, передаваемые в США без уведомления РКН о трансграничной передаче

Прослойка между этими зонами — техника обезличивания. Согласно securegpt.ru, обезличенные данные выходят из-под действия 152-ФЗ при условии, что восстановить идентичность субъекта по оставшимся атрибутам невозможно. На практике это означает маскирование имён, телефонов и адресов перед отправкой в API внешней модели.

Четыре сценария, где on-prem действительно обязателен

Существуют отраслевые контексты, в которых архитектура с локальным развёртыванием модели — не паранойя, а требование регулятора или невозможность иначе обойти правовые риски.

Банки и финансовые организации. ЦБ РФ Положение № 787-П устанавливает требования к внутреннему контролю ИТ-рисков. Статья 395-1 ФЗ «О банках» — банковская тайна — запрещает передачу информации о клиентах и операциях третьим лицам без согласия. Кредитные истории регулируются отдельным 353-ФЗ. На практике любой банк, который хочет внедрить AI-агента в кредитный процесс или клиентский сервис, обязан использовать решения, одобренные ЦБ, либо on-prem-развёртывание. Claude или OpenAI API напрямую — невозможны.

Медицина. Приказ Минздрава № 911н и Постановление Правительства № 1119 (уровень защищённости УЗ-1) устанавливают требования к медицинским информационным системам. AI-ассистент для ведения электронных медицинских карт обязан работать в аттестованной МИС с интеграцией в ЕГИСЗ. Обход невозможен через организационные меры — данные о здоровье относятся к специальным категориям ПДн по ст. 10 152-ФЗ, и облачные зарубежные API исключены без исключений.

Государственные закупки с элементами гостайны. Для систем, работающих с документами, составляющими государственную тайну, требуется сертификация ФСТЭК и/или ФСБ. Ни один публичный облачный AI-провайдер в 2026 году такой сертификацией не обладает. Для обычных тендеров по 44-ФЗ / 223-ФЗ облако формально допустимо, но начиная с 1 января 2026 применяются единые защитные меры вне зависимости от категории закупок (поправки к 44-ФЗ, вступившие в силу с 01.01.2026). Готовящийся реестр доверенных моделей, который войдёт в AI-закон, сделает on-prem-сертифицированные решения обязательными для государственных заказчиков.

Массовые физлица без обезличивания. Компании, которые обрабатывают заявки конечных потребителей — электронная коммерция, телемедицина, кредитование, — и хотят пропускать необезличенные данные через AI-модель, юридически не могут использовать зарубежный облачный API без уведомления РКН о трансграничной передаче и заключения договора с провайдером в стране, находящейся в Перечне разрешённых направлений. В 2026 году США в этом перечне нет. Германия (AWS Bedrock EU, регион Frankfurt) — есть, что открывает одну из рабочих схем, но требует отдельной юридической проверки.

Три сценария, где облако работает законно

B2B-сервис с данными юрлиц. Автоматизация закупок, управление парком техники, тендерный мониторинг, классификация входящих обращений от корпоративных клиентов. Если в системе хранятся только юридические реквизиты контрагентов — это не персональные данные. ДПО (договор поручения обработки ПДн) между компанией-разработчиком и клиентом требуется для фиксации ответственности, но сам по себе не запрещает облако. Типичная конструкция: разработчик выступает обработчиком, клиент — оператором, при этом в приложении к договору прямо указано, что обработке подлежат только данные юрлиц, и зафиксировано, что ФИО конкретных людей маскируются перед отправкой в API.

Обезличенный голосовой AI. Запись и транскрипция звонков — часто вызывает тревогу, но при правильном оформлении работает через облако. Требуется три меры: уведомление клиента до начала разговора («разговор записывается и обрабатывается автоматической системой»), обезличивание имён и телефонов перед отправкой в LLM, хранение необезличенной записи только на российском сервере. Практика уведомления клиентов о записи разговоров давно отработана колл-центрами — достаточно фразы до начала разговора с упоминанием автоматической обработки. AI-слой добавляет к этому только требование об обработчике.

Строительство и спецтехника (B2B-коммуникация). Запросы от компаний-заказчиков, координация субподрядчиков, управление объектами — в основе лежат данные юрлиц. Основной риск — данные о работниках (ФИО, паспортные данные, данные иностранных граждан по 115-ФЗ). Пока AI-агент работает с координацией заявок и операционными данными, а не с кадровым учётом, облачный стек совместим с 152-ФЗ. При появлении кадровых задач — граница проходит по типу данных, а не по отрасли.

Сравнительная таблица: что реально нужно по отраслям

Отрасль	Тип данных	Можно облако?	Что нужно минимально
Спецтехника B2B	Данные юрлиц + заявки	Да	ДПО + обезличивание ФИО ЛПР
Строительство (субподрядчики)	Юрлица + данные работников	Частично	ДПО + обезличивание; кадровые данные — отдельно
Оптовая торговля B2B	Юрлица + корп. контакты	Да	ДПО + стандартная политика ПДн
Розничная e-commerce	Данные физлиц (адреса, телефоны)	С оговорками	Обезличивание + ДПО + уведомление РКН
Автодилеры (ПТС + кредиты)	ПДн физлиц + кредитные данные	Нет для кредитов	On-prem или GigaChat Enterprise; 395-1 ФЗ + 353-ФЗ
Медицина	Медицинские данные	Нет	On-prem + МИС + ЕГИСЗ
Банки	Банковская тайна	Нет	On-prem + требования ЦБ
Госзакупки с гостайной	Сведения ограниченного доступа	Нет	ФСТЭК/ФСБ сертификация

GigaChat Enterprise: когда он действительно нужен

GigaChat Enterprise — не «импортозамещение ради галочки», а реальный production-вариант для сценариев из красной зоны. Официальная страница b2b.giga.chat описывает три формата развёртывания: облако Сбера, гибрид (данные на серверах клиента, модель в приватном облаке Сбера), локальная установка на мощностях клиента. Гибридный формат — наиболее распространённый для compliance-sensitive B2B: данные физически не покидают периметр клиента, а модель работает в изолированном облачном сегменте.

Цена вопроса: согласно документации GigaChat API, GigaChat 2 Pro стоит 500 ₽ за миллион токенов (около $5.55), что в 10–15 раз дешевле Claude Sonnet. GigaChat 3.1 Lightning — self-hosted GGUF-модель, доступная для локального запуска без API-расходов. Разрыв в качестве относительно лидирующих западных моделей на аналитических задачах реален; на задачах диспетчеризации, классификации и суммаризации на русском языке он значительно меньше.

Четыре инженерных ограничения, которые стоит проверить перед production-внедрением: (1) качество function calling на длинных цепочках инструментов — документация 2026 года существенно улучшилась, но тесты на реальных сценариях остаются обязательными; (2) latency гибридного развёртывания — добавляет задержку по сравнению с прямым облачным API; (3) context window — актуальные характеристики меняются с каждым релизом, сверяться с документацией SberDevices на момент старта проекта; (4) observability — для enterprise on-prem нужен отдельный logging-слой, который обычно не идёт из коробки.

Договорная конструкция: минимум для запуска

Неочевидная часть compliance в B2B AI — не выбор модели, а договорная структура. Согласно практике, описанной RTM Group, для AI-сервисов корректная конструкция — договор возмездного оказания услуг, а не лицензионный договор: экземпляр ПО пользователю не передаётся, сервис оказывается на стороне провайдера, лицензия юридически ничтожна.

Ключевой инструмент — **договор поручения обработки ПДн (ДПО)**. Он фиксирует: кто является оператором (клиент, в чьих интересах данные), кто — обработчиком (разработчик AI-сервиса), какие именно категории данных передаются, каков максимальный срок хранения. Шаблоны ДПО для B2B-сервисов включают стандартные блоки, адаптируемые к конкретному проекту. Практика сопровождения ПДн показывает, что юридическая работа по оформлению ДПО и адаптации политики конфиденциальности для одного B2B-клиента обычно стоит 25–40 тыс. ₽ у специализированного юриста.

Минимальный пакет, с которым можно запускать AI-агента в B2B-эксплуатацию: 1. **ДПО между разработчиком и клиентом** с перечнем передаваемых категорий данных 2. **Политика конфиденциальности клиента** с разделом об AI-обработке 3. **Уведомление РКН** (если клиент ещё не подавал — подаётся до начала обработки через Госуслуги) 4. **Уведомление конечных пользователей** о взаимодействии с AI (стандартный текст в начале чата или звонка)

Дополнительно, при использовании зарубежного облачного API с любыми ПДн: процедура обезличивания с документированием того, какие поля маскируются перед отправкой, и кто несёт ответственность за полноту маскирования.

Что меняет закон об AI (с 2027 года)

В марте 2026 года Минцифры опубликовало законопроект «Об основах государственного регулирования применения технологий ИИ». По материалам vc.ru и разбору на Habr, закон рамочный, вступает в силу с 1 сентября 2027 года. Три пункта важны для команд, которые проектируют AI-системы сегодня.

Обязанность информировать. Статья 9.1 устанавливает: компания обязана уведомить пользователя о том, что с ним взаимодействует AI, до начала взаимодействия. Это уже сейчас хорошая практика; с 2027 — правовое требование. Чат-бот, который выдаёт себя за человека, станет нарушением закона.

Реестр доверенных моделей. Один из ключевых механизмов, который обсуждается в проекте — реестр AI-моделей, прошедших сертификацию для работы в государственных и критических информационных системах. Для частного B2B это требование может не применяться напрямую, но создаёт косвенное давление: клиенты из регулируемых отраслей будут всё чаще спрашивать о наличии сертификации.

Распределение ответственности. Закон вводит цепочку: разработчик модели → оператор AI-системы → пользователь. Ответственность за вред, причинённый AI-выводом, распределяется «соразмерно степени вины». Для B2B AI-провайдера это означает: договор должен явно фиксировать, на ком лежит ответственность за конкретные решения системы, иначе суд будет распределять её по своему усмотрению.

Главное

- Большинство B2B AI-проектов работает с данными юрлиц — это не персональные данные по 152-ФЗ, и on-prem для них не требуется.
- On-prem обязателен в четырёх сценариях: банки и финансы, медицина, госзакупки с гостайной, необезличенные данные физических лиц.
- Для серой зоны (деловые контакты, записи звонков, адреса доставки) достаточно ДПО + обезличивания + уведомления РКН — облако работает законно.
- Штрафы за утечку выросли до 500 млн ₽, но само по себе использование облачного AI без ПДн нарушением не является.
- GigaChat Enterprise гибрид — практичный выбор для compliance-sensitive B2B; выигрывает у YandexGPT по изолированности данных, уступает Claude по качеству на аналитических задачах.
- AI-закон (с 2027): уведомлять пользователей об AI-взаимодействии, готовиться к реестру доверенных моделей, фиксировать ответственность в договоре уже сейчас.

FAQ

Что такое ДПО и чем он отличается от обычного договора?

Договор поручения обработки персональных данных (ДПО) — это обязательный документ по ст. 6 ч. 3 152-ФЗ, который заключается, когда оператор (клиент) привлекает третью сторону (разработчика AI) для обработки ПДн. В отличие от обычного NDA или договора оказания услуг, ДПО фиксирует именно правовые основания для доступа к данным, перечень обрабатываемых категорий, запрет использования данных в иных целях и срок хранения. Без ДПО разработчик AI-сервиса формально является незаконным обработчиком ПДн.

Данные юрлиц точно не персональные данные?

Точнее — не всегда. Реквизиты самой организации (ИНН, ОГРН, юридический адрес) — не ПДн. Но ФИО директора, email «ivan.petrov@company.ru», корпоративный мобильный номер конкретного менеджера — это уже информация, позволяющая идентифицировать физическое лицо. Практически это означает:

обращения от юрлиц обрабатываются свободнее, но ФИО контактных лиц лучше маскировать перед отправкой в облачный API — это снимает 90% вопросов.

Обезличивание: какой минимум защищает?

Стандартный минимум для B2B AI, работающего с голосом или текстом: замена имён и отчеств на токены типа «[PERSON_1]», маскирование телефонных номеров (первые 6 цифр + маска), удаление адресов проживания. Этого достаточно, чтобы данные, отправляемые в облачный LLM, формально стали обезличенными по критериям РКН. Детальные требования к методам обезличивания установлены Приказом РКН № 996 от 5 сентября 2013 года.

Когда уведомление о взаимодействии с AI не нужно?

Сейчас — когда AI работает полностью во внутреннем контуре клиента без прямого контакта с его клиентами. Например, AI-агент, который обрабатывает входящие заявки и готовит черновики ответов для менеджера — контакт происходит между менеджером и клиентом, а не между AI и клиентом. С 2027 года, после вступления AI-закона в силу, правило об информировании станет обязательным при любом прямом взаимодействии AI с конечным пользователем.

Как проверить, что ваша текущая архитектура не нарушает 152-ФЗ?

Три вопроса для быстрой диагностики: (1) Какие категории данных физических лиц видит AI-модель до маскирования? Если ответ «никакие» — вы в зелёной зоне. (2) Есть ли подписанный ДПО с каждым клиентом, данные которого обрабатывает ваш AI? Если нет — это первоочередной риск. (3) Куда физически уходят данные при обращении к API модели — в РФ или за рубеж? Если за рубеж и среди данных есть ПДн физлиц без обезличивания — нужно уведомление РКН о трансграничной передаче.

Ещё по теме: Не GigaChat против Claude. Моноархитектура против маршрутизатора — как выбирать LLM-стек по архитектурным, а не закупочным критериям. Регламент как код — как превратить compliance-инструкции в исполняемые правила.