

Персональные данные граждан РФ: почему группе компаний нужен локальный AI-контур

Юридические запреты, штрафы и практическое обоснование внедрения ABS

Адресат: собственникам, акционерам и генеральным директорам групп компаний

Дата подготовки: 7 июля 2026 г.

Назначение документа: краткое юридико-маркетинговое обращение к собственникам и руководителям предприятий о необходимости локального контура обработки данных и AI-инструментов.

Главный тезис: когда персональные данные граждан РФ, данные сотрудников, клиентские базы и корпоративные документы попадают в зарубежные облака или внешние AI-сервисы, собственник получает не технологическое ускорение, а юридический, регуляторный и репутационный риск.

1. Ключевой вывод для собственника

Управленческий вывод

Российское законодательство не вводит абсолютный запрет на любую трансграничную передачу персональных данных. Но оно прямо запрещает выполнять ключевые операции с персональными данными граждан РФ с использованием баз данных, находящихся за пределами РФ, и устанавливает специальный разрешительный/уведомительный режим трансграничной передачи. Для собственника безопасная модель - локальный контур обработки данных и локальный AI-контур ABS.

Для обычной группы компаний основной риск возникает не только при “продаже” или намеренной передаче данных иностранной стороне. Риск возникает уже тогда, когда HR-база, клиентская база, база подрядчиков, CRM, корпоративная почта, документы, заявки, таблицы или промпты с персональными данными фактически обрабатываются через иностранную облачную платформу, зарубежный SaaS или внешнюю AI-модель.

2. Что прямо запрещено или недопустимо

Запрет / ограничение	Норма закона	Практический смысл для компании
Не допускается запись, систематизация, накопление, хранение, уточнение и извлечение персональных данных граждан РФ с использованием баз данных за пределами РФ.	152-ФЗ, ст. 18 ч. 5; 149-ФЗ, ст. 16 ч. 4 п. 7	Нельзя делать иностранное облако или зарубежную SaaS-систему основной базой для российских ПДн. Первичный контур должен быть в РФ.
Нельзя начинать трансграничную передачу ПДн без предварительного уведомления Роскомнадзора.	152-ФЗ, ст. 12 ч. 3; официальный портал РКН	Передача ПДн в иностранную CRM, helpdesk, HR-сервис, маркетинговую платформу или внешнюю AI-модель требует предварительной юридической процедуры.
Трансграничная передача может быть запрещена или ограничена уполномоченным органом.	152-ФЗ, ст. 12 ч. 8-12	Если Роскомнадзор запретил или ограничил передачу, продолжать ее нельзя; ранее переданные данные должны быть уничтожены иностранным получателем в установленном порядке.
Работодатель не вправе сообщать персональные данные работника третьей стороне без письменного согласия, кроме случаев, предусмотренных законом.	ТК РФ, ст. 88	Данные сотрудников нельзя бесконтрольно выгружать подрядчикам, зарубежным сервисам, AI-платформам и внешним аналитическим системам.
Нельзя допускать неправомерную передачу, предоставление, распространение или доступ к ПДн.	КоАП РФ, ст. 13.11 ч. 12-18	Утечка через иностранный сервис, облако, внешнего подрядчика или AI-инструмент может привести к многомиллионным и оборотным штрафам.

3. Типовые действия, которые создают риск для собственника

- **Загрузка клиентской базы в зарубежные маркетинговые сервисы.** Даже если цель - рассылка, аналитика или скоринг, это может быть трансграничной передачей и/или нарушением локализации, если база фактически ведется за рубежом.
- **Использование иностранной CRM как основной базы ПДн граждан РФ.** Если запись, хранение, обновление и извлечение российских ПДн происходят за пределами РФ, возникает прямой риск по 152-ФЗ и 149-ФЗ.
- **Отправка кадровых документов во внешние AI-сервисы.** Паспорта, трудовые договоры, больничные, зарплатные таблицы, резюме, оценки KPI и переписка сотрудников являются зоной повышенного риска.

- **Передача доступа иностранному подрядчику к корпоративным системам.** Даже без выгрузки файла доступ к базе может квалифицироваться как предоставление/доступ к ПДн.
- **Использование внешних AI-чатов для анализа договоров и внутренних документов.** Если документы содержат ФИО, телефоны, email, паспортные данные, кадровую информацию или сведения о клиентах, это уже не “просто текст”, а потенциальная обработка ПДн.

4. Ответственность и штрафы

Нарушение	Норма	Штраф / последствия
Нарушение требования локализации баз ПДн граждан РФ	КоАП РФ, ст. 13.11 ч. 8	Юрлица: 1-6 млн ₽; должностные лица: 100-200 тыс. ₽; граждане: 30-50 тыс. ₽.
Повторное нарушение локализации	КоАП РФ, ст. 13.11 ч. 9	Юрлица: 6-18 млн ₽; должностные лица: 500-800 тыс. ₽; граждане: 50-100 тыс. ₽.
Обработка ПДн в случаях, не предусмотренных законом, либо несовместимо с целями сбора	КоАП РФ, ст. 13.11 ч. 1	Юрлица: 150-300 тыс. ₽; должностные лица: 50-100 тыс. ₽; граждане: 10-15 тыс. ₽.
Нет письменного согласия, когда оно обязательно	КоАП РФ, ст. 13.11 ч. 2	Юрлица: 300-700 тыс. ₽; должностные лица: 100-300 тыс. ₽; граждане: 10-15 тыс. ₽.
Неправомерная передача/доступ к ПДн: 1 000-10 000 субъектов или 10 000-100 000 идентификаторов	КоАП РФ, ст. 13.11 ч. 12	Юрлица: 3-5 млн ₽; должностные лица: 200-400 тыс. ₽; граждане: 100-200 тыс. ₽.
Неправомерная передача/доступ к ПДн: 10 000-100 000 субъектов или 100 000-1 млн идентификаторов	КоАП РФ, ст. 13.11 ч. 13	Юрлица: 5-10 млн ₽; должностные лица: 300-500 тыс. ₽; граждане: 200-300 тыс. ₽.
Неправомерная передача/доступ к ПДн: более 100 000 субъектов или более 1 млн идентификаторов	КоАП РФ, ст. 13.11 ч. 14	Юрлица: 10-15 млн ₽; должностные лица: 400-600 тыс. ₽; граждане: 300-400 тыс. ₽.
Повторная крупная утечка/неправомерная передача	КоАП РФ, ст. 13.11 ч. 15	Юрлица: 1-3% совокупной выручки/капитала, но не менее 20 млн ₽ и не более 500 млн ₽.
Неправомерная передача специальных категорий ПДн	КоАП РФ, ст. 13.11 ч. 16	Юрлица: 10-15 млн ₽; должностные лица: 1-1,3 млн ₽; граждане: 300-400 тыс. ₽.
Неправомерная передача биометрических ПДн	КоАП РФ, ст. 13.11 ч. 17	Юрлица: 15-20 млн ₽; должностные лица: 1,3-1,5 млн ₽; граждане: 400-500 тыс. ₽.
Повторная утечка специальных/биометрических ПДн	КоАП РФ, ст. 13.11 ч. 18	Юрлица: 1-3% выручки/капитала, но не менее 25 млн ₽ и не более 500 млн ₽.

5. Почему собственнику выгоден локальный AI-контур ABS

ABS следует позиционировать не как “ещё один AI-чат”, а как локальную корпоративную операционную систему, которая позволяет использовать искусственный интеллект без вывода чувствительных данных за пределы контролируемой инфраструктуры компании.

Риск без локального контура	Как закрывает ABS
Данные уходят в зарубежные LLM, SaaS, облака и подрядческие сервисы.	Обработка внутри локального или российского инфраструктурного контура заказчика.
HR, финансы, клиентская база и договоры смешиваются в неуправляемых внешних сервисах.	Разделение контуров: ПДн, коммерческая тайна, управленческие документы, база знаний, контент.
Непонятно, кто и когда получил доступ к данным.	Ролевая модель доступа, журналирование действий, управляемые права пользователей и агентов.
Риск передачи лишних данных при работе сотрудников с AI.	Корпоративные политики, запрет внешней отправки ПДн и безопасные сценарии работы с документами.
Собственник зависит от иностранных правил, блокировок и изменения доступа к сервисам.	Технологическая независимость: собственная база знаний, локальные модели, российская инфраструктура, контролируемые интеграции.

6. Готовая формулировка для коммерческого предложения ABS

Рекомендуемый текст

ABS создаёт локальный AI-контур для российской группы компаний: персональные данные сотрудников и клиентов, внутренняя документация, договоры, финансовая и управленческая аналитика обрабатываются внутри контролируемой инфраструктуры заказчика, без передачи в зарубежные облака и внешние AI-сервисы.

Юридически корректная формула: не “закон всегда запрещает любую передачу данных за рубеж”, а “закон требует локализовать ключевые операции с ПДн граждан РФ в РФ, а трансграничную передачу проводить только по специальной процедуре; для собственника безопаснее и управляемее строить локальный AI-контур”.

Нормативные ссылки

Ссылки ниже кликабельны в электронной версии PDF. Основной источник сводных редакций - КонсультантПлюс; для процедур трансграничной передачи дополнительно указан официальный портал Роскомнадзора.

1. [152-ФЗ, ст. 18 ч. 5 - локализация баз персональных данных](#) — источник: consultant.ru
2. [152-ФЗ, ст. 12 - трансграничная передача персональных данных](#) — источник: consultant.ru
3. [Роскомнадзор - уведомление о намерении осуществлять трансграничную передачу ПДн](#) — источник: pd.rkn.gov.ru
4. [149-ФЗ, ст. 16 - защита информации и локализация баз ПДн](#) — источник: consultant.ru
5. [ТК РФ, ст. 88 - передача персональных данных работника](#) — источник: consultant.ru
6. [КоАП РФ, ст. 13.11 - ответственность за нарушения в области персональных данных](#) — источник: consultant.ru

Оговорка: документ является информационно-аналитическим и маркетинговым материалом для обсуждения внедрения локального AI-контура ABS. Он не заменяет индивидуальное юридическое заключение, аудит ИСПДн, КИИ, режима коммерческой тайны, гостайны и требований ФСТЭК/ФСБ для конкретного предприятия.