



Базовый чек-лист по комплаенсу персональных данных при использовании ИИ в РФ [05.10.2026]

Порядок использования чек-листа:

1. **До запуска ИИ** (облако, API, локальная модель, агент) чек-лист заполняют ответственный за использование ИИ, DPO (ответственный за обработку ПД) и специалист по информационной безопасности (ИБ).
2. **Оценку повторяют** при плановой проверке и до смены модели, поставщика, тарифа, состава ПД, стран передачи или доступа ИИ.
3. **Да** ставится, только если верно все в строке, иначе **Част.** или **Нет**. **н/п** (не применимо) ставится с причиной в комментарии.
4. **В комментариях** указываются подтверждение проверки (документ, договор, снимок экрана), ограничения и срок исправления.
5. **Обязательны** все пункты, кроме рекомендованных 2.4* и 4.4*. **Нет** по обязательному пункту запрещает работу с ИИ.
6. **Част.** по обязательному пункту разрешает ИИ только для задач и данных, где все обязательные пункты выполнены.
7. **Ссылки** в квадратных скобках относятся к 152-ФЗ, если не указан другой акт.

№	Критерий проверки	Да	Част.	Нет	н/п	Комментарий
I. Сценарий использования и правовые основания						
1.1	Описано, зачем нужен ИИ, какие ПД в него попадают (запросы, ответы, файлы, история чатов) и куда они уходят дальше. Назначен ответственный. [ст.3, 5, 18.1]	○	○	○	○	
1.2	Для каждой цели есть правовое основание (согласие, договор, закон и др.) и его условия выполнены. Отдельно проверены передача ПД поставщику, обучение на ПД и данные, полученные не от самого человека. [ст.6; ч.8 ст.9]	○	○	○	○	
1.3	Если есть специальные категории ПД (например, о здоровье), биометрия для установления личности, ПД работников или охраняемая тайна, DPO подтвердил основание, обычно письменное согласие. [ст.7, 10–11; ТК ст.88]	○	○	○	○	
1.4	Из запросов и файлов убраны ПД, не нужные для задачи. При обезличивании проверено, что людей нельзя узнать без дополнительных сведений. Замена ФИО кодом сама по себе не снимает требований к ПД. [ст.5; приказ РКН № 140]	○	○	○	○	
1.5	Утвержден регламент работы с ИИ. Если нужно, обновлены политика, сведения в реестре операторов РКН и уведомления людям. Работники знают разрешенные сервисы и ПД и что делать, если загрузили лишнее. [ст.18, 18.1, 22]	○	○	○	○	
II. Поставщик ИИ и что он делает с ПД (если ПД доступны кому-то вне компании)						
2.1	Известны поставщик и другие получатели ПД (например, его подрядчики). Для каждого понятно, работает ли он только по вашему заданию (поручение) или и в своих целях, например обучает свою модель. [п.2 ст.3; ст.6]	○	○	○	○	
2.2	Если поставщик работает по поручению, в договоре есть все условия поручения (перечень ПД, действий и целей, конфиденциальность, защита ПД, документы по запросу, сообщение об утечках). [ч.3 ст.6]	○	○	○	○	
2.3	Проверено, хранит ли сервис запросы и ответы, учится ли на них и кто их видит. Ничего из этого не выходит за цели и основания пунктов 1.1 и 1.2. [ст.5–7]	○	○	○	○	
2.4*	Используется корпоративный тариф, а не личные бесплатные аккаунты. Настройки обучения и срок хранения сохранены, например снимком экрана.	○	○	○	○	
III. Хранение ПД в РФ и передача за рубеж						
3.1	Если ИИ собирает ПД граждан РФ (например, чат-бот на сайте), используются только базы данных в РФ, исключения подтверждает DPO. [ч.5 ст.18]	○	○	○	○	
3.2	Если ПД передаются за рубеж или к ним есть доступ из-за рубежа (ТПД), известны страны и получатели. До уведомления РКН от получателей получены сведения о них и о защите ПД. [чч.4–5 ст.12]	○	○	○	○	
3.3	До ТПД в РКН подано отдельное уведомление, если оно требуется. В страны вне перечня РКН передача начата не раньше чем через 10 рабочих дней после поступления уведомления, а при приостановке срока позже. Запреты и ограничения РКН соблюдаются. [чч.3, 7–11 ст.12]	○	○	○	○	
IV. Защита ПД и эксплуатация ИИ						
4.1	Со специалистами по ИБ оценен вред людям и проверена защита ПД, для ИСПД определен уровень защищенности. ИИ видит и делает только нужное для задачи (например, агент читает письма, но не отправляет). [ст.18.1, 19; ПП № 1119]	○	○	○	○	
4.2	Заданы сроки хранения ПД. Неточные ПД исправляются. Запросы людей на доступ, исправление и удаление ПД выполняются во всех местах хранения, включая историю чатов, файлы у поставщика и резервные копии. [ст.5, 14, 20–21]	○	○	○	○	
4.3	Решения о правах людей (например, отказ в услуге) принимает человек, а без человека только с письменного согласия или по закону, с правом возразить. О решениях только по выводам ИИ не принимаются. [ст.16; ТК ст.86]	○	○	○	○	
4.4*	На разрешенных тестовых данных (например, вымышленных) проверено, что ИИ не выдает чужие ПД, не открывает закрытые файлы и не искажает сведения о людях. Результаты записаны. [ч.6 ст.5; пп.4, 9 ч.2 ст.19]	○	○	○	○	