

Чек-лист проверки data controls для enterprise-агента

PDF-чек-лист для [downloads/checklist.pdf](#): его можно использовать перед пилотом агентного приложения на OpenAI Platform или как структуру вопросов к поставщику ИИ-инструмента.

Карта данных

- Опишите входные данные, model call, hosted tool, container filesystem, external MCP, логи и региональные настройки.
- Разделите customer content, application state, abuse monitoring logs и данные, уходящие во внешние сервисы.
- Проверьте, какие артефакты создаются в процессе работы агента и где они должны храниться после выполнения задачи.

Retention и режимы OpenAI

- Проверьте, применим ли Zero Data Retention к вашим endpoints, моделям, tools и типам данных.
- Не трактуйте ZDR как обещание, что данные нигде и никогда не сохраняются.
- Отдельно зафиксируйте, какие данные попадают в abuse monitoring logs и какие сроки хранения описаны для вашего сценария.

Hosted tools и контейнеры

- Определите, какие файлы можно передавать в контейнер, а какие запрещены внутренней политикой.
- Опишите lifecycle временных файлов, промежуточных таблиц, результатов вычислений и логов выполнения.
- Сохраняйте бизнес-критичные артефакты в управляемых системах клиента, а не только во временной среде инструмента.

MCP и внешние сервисы

- Разделите hosted tools OpenAI, local tools клиента и third-party MCP по уровням доверия.
- Проверьте условия retention, доступа и аудита у внешних MCP-серверов и коннекторов.
- Для операций, которые меняют состояние внешних систем, настройте allowlists и human approval.

Data residency и ограничения

- Проверьте data residency на уровне конкретного endpoint, модели, capability и региона.
- Различайте региональное хранение и региональную обработку данных.
- Для российских организаций отдельно проверьте правовую доступность сервиса и конкретных controls, не делая выводов только по общей документации.