

Checklist AI Act 2026

CRITERIO DIGITALE / ПРАКТИЧЕСКИЙ ИНСТРУМЕНТ

Русская редакция

Быстрый маршрут + подробная проверка

Версия 1.0

Актуально на 1 сентября 2026

Этот документ помогает провести первичную рабочую проверку конкретного сценария использования AI:

- ☐ определить возможную связь с AI Act;
- ☐ понять свою роль;
- ☐ выбрать нужный маршрут;
- ☐ собрать факты и документы;
- ☐ увидеть вопросы, которые требуют специалиста.

Проверяйте один сценарий использования за раз. Одна организация может одновременно выступать в разных ролях для разных систем.

Это не юридическое заключение и не подтверждение соответствия AI Act.

Автор: Татьяна Мирошина

Проект: Criterio Digitale

Версия 1.0 · актуально на 2026-09-01

Сначала определите, как ваш сценарий связан с ЕС

Русский язык этого документа не означает, что вы находитесь вне ЕС.

Русскоязычный читатель может работать в Италии, Германии или другой стране ЕС; управлять европейской компанией; поставлять AI из третьей страны на рынок ЕС; работать между несколькими юрисдикциями или изучать европейское регулирование только для информации.

Проверяйте не язык и гражданство, а факты конкретного сценария.

А. Ваша организация использует AI в ЕС

Организация, использующая систему под своей ответственностью, учреждена или находится в ЕС.

Статус: СВЯЗЬ С ЕС ПОДТВЕРЖДЕНА

Подтверждён только входной территориальный критерий. Это ещё не означает, что к сценарию применимы все положения AI Act или что организация им соответствует.

Дальше: определите роль и перейдите к вопросам на странице 3.

В. Организация находится вне ЕС, но возможна связь с европейским рынком

ДЕЙСТВУЮЩАЯ НОРМА

Проверьте, происходит ли хотя бы одно из следующего:

AI-система или GPAI-модель выводится на рынок ЕС;
AI-система вводится в эксплуатацию в ЕС; результат, произведённый AI-системой, используется в ЕС;
производитель под своим именем/товарным знаком выводит AI-систему вместе с продуктом на рынок либо вводит их в эксплуатацию;
организация участвует в европейской цепочке поставки как импортёр, дистрибьютор или уполномоченный представитель;
продукт, договоры и фактическая поставка создают другую конкретную связь с рынком ЕС.

Статус: ВОЗМОЖНА ПРИМЕНИМОСТЬ

Нужны факты о продукте, поставке, договорной цепочке, назначении и использовании результатов.

Европейский клиент сам по себе не доказывает применимость AI Act. Нужно проверить, что именно поставляется, куда выводится продукт, где он вводится в эксплуатацию и где используется результат.

Дальше: маршрут D и, при необходимости, маршрут В или С.

С. Очевидной связи с ЕС пока не выявлено

Нет вывода AI-продукта на рынок ЕС, ввода системы в эксплуатацию, участия в цепочке поставки или использования результата AI-системы в ЕС.

Статус: ИНФОРМАЦИОННЫЙ РЕЖИМ

Документ можно использовать для понимания европейского подхода и подготовки к возможной работе с рынком ЕС.

Этот статус не означает окончательного вывода «AI Act не применяется». Если факты, рынок или цепочка поставки изменятся, территориальную проверку нужно повторить.

D. Вы работаете между несколькими юрисдикциями

Разделите проверку:

- ☐ 1. по каждому сценарию использования;
- ☐ 2. по каждой организации;
- ☐ 3. по каждой роли;
- ☐ 4. по каждой стране или рынку, с которыми связан сценарий.

Язык команды, гражданство владельца и место регистрации компании могут не совпадать с рынком, местом эксплуатации и страной использования результата.

Статус: ТРЕБУЕТ ПРОВЕРКИ

Составьте короткую записку с фактами и передайте её специалисту, если территориальная связь остаётся неоднозначной.

Основание: S1 — Articles 2–3 и Recital 22.

Ответьте на восемь вопросов

Для неизвестного ответа выбирайте «Требуется проверки». Не заменяйте отсутствие фактов предположением.

1. Организация, использующая систему, учреждена или находится в ЕС?

- ☐ Да → связь с ЕС подтверждена; продолжайте с вопроса 3.
- ☐ Нет → вопрос 2.
- ☐ Требуется проверки → маршрут D.

2. Есть ли у деятельности вне ЕС конкретная связь с рынком или использованием в ЕС?

Проверьте вывод AI-системы или GPAI-модели на рынок ЕС, ввод в эксплуатацию, использование результата и европейскую цепочку поставки.

- ☐ Да или возможно → маршрут D.
- ☐ Нет очевидной связи → информационный режим.
- ☐ Требуется проверки → маршрут D + legal.

3. Вы используете готовый AI-сервис или создаёте и поставляете собственное решение?

- ☐ Только используем готовый сервис → обычно маршрут A; затем проверьте роль.
- ☐ Собираем, брендируем или поставляем решение → маршрут C.
- ☐ Создаём или поставляем модель общего назначения → маршрут C, блок GPAI.
- ☐ Требуется проверки → страницы 6 и 13.

4. Система принимает или поддерживает решения о людях?

Примеры: найм, образование, кредит, страхование, доступ к услугам, правоохранительная деятельность, миграция.

- ☐ Да → маршрут B.
- ☐ Нет → продолжайте.
- ☐ Требуется проверки → маршрут B до уточнения.

5. Есть ли сигнал запрещённой практики из Article 5?

- ☐ Да или возможно → остановить соответствующее использование; страница 7; legal.
- ☐ Нет → продолжайте.
- ☐ Требуется проверки → не запускать чувствительную функцию до оценки.

6. Система общается с людьми или создаёт синтетический публичный контент?

Проверьте чат-интерфейс, deepfake, синтетические текст, аудио, изображения и видео, распознавание эмоций и биометрическую категоризацию.

- ☐ Да → страница 11.
- ☐ Нет → продолжайте.
- ☐ Требуется проверки → запросите документацию поставщика.

7. Используются персональные или чувствительные данные либо возможны существенные последствия для прав людей?

- ☐ Да → страница 14; DPO/legal при необходимости.
- ☐ Нет → продолжайте.
- ☐ Требуется проверки → составьте карту данных.

8. Вы изменили название, назначение или существенные характеристики системы?

- ☐ Да или возможно → страница 13; проверка Article 25.
- ☐ Нет → сохраните подтверждающие факты.
- ☐ Требуется проверки → сравните исходную документацию поставщика со своим решением.

Рабочие маршруты

МАРШРУТ А

Маршрут А — Обычное использование AI

Когда выбирать: готовый AI-инструмент используется для черновиков, анализа, поиска идей, внутренней поддержки или других обычных задач без очевидного существенного воздействия на людей.

Читайте: 4, 6, 9, 10, 11, 14, 19.

Результат: карточка сценария, меры AI-грамотности, правила данных и человеческой проверки, вывод по Article 50.

Передача специалисту: чувствительные данные, сложная автоматизация, неопределённая роль, права третьих лиц.

[Далее](#)

МАРШРУТ В

Маршрут В — Решения о людях или существенное воздействие

Когда выбирать: система влияет на найм, образование, кредит, страхование, доступ к важным услугам, правоохранительную деятельность, миграцию или другие чувствительные решения.

Читайте: 4, 6–8, 11, 12, 14, 19.

Результат: зафиксированные проверки Article 5, Article 6, данных, DPIA и FRIA.

Передача специалисту: запрещённые практики, high-risk классификация, значимые решения о людях.

[Далее](#)

МАРШРУТ С

Маршрут С — Создаю или поставляю AI-решение

Когда выбирать: вы собираете продукт на чужой модели, продаёте AI-систему под своим именем, меняете назначение системы или создаёте собственную модель.

Читайте: 4, 6–8, 11–15, 19.

Результат: карта ролей и цепочки поставки, проверка Article 25, перечень документации и обязанностей поставщика.

Передача специалисту: квалификация продукта, договоры, high-risk, GPAI и ответственность в цепочке поставки.

[Далее](#)

МАРШРУТ D

Маршрут D — Организация вне ЕС / проверка территории

Когда выбирать: организация находится вне ЕС, но AI-продукт, эксплуатация, результат или цепочка поставки могут быть связаны с ЕС.

Читайте: 2–4, 6, затем А, В или С по характеру деятельности.

Результат: короткая записка о территориальных фактах и перечень неизвестных обстоятельств.

Передача специалисту: неоднозначное применение Article 2, несколько стран, сложная договорная или дистрибьюторская цепочка.

Маршруты могут сочетаться. Например, компания вне ЕС, поставляющая в ЕС инструмент подбора кандидатов, начинается с D и продолжает по С и В.

[Далее](#)

Что должно остаться после проверки

- ☐ Описан один конкретный сценарий использования
- ☐ → Карточка: задача, система, люди, данные, результат, владелец процесса.
- ☐ Зафиксированы факты о связи с ЕС
- ☐ → Короткая территориальная записка без общего вывода о полном соответствии.
- ☐ Сформулирована рабочая гипотеза о роли
- ☐ → Deployer, provider или другая роль с указанием неизвестных фактов.
- ☐ Собраны документы поставщика
- ☐ → Назначение, ограничения, инструкции, условия, технические и прозрачные материалы.
- ☐ Проверены возможные сигналы Article 5
- ☐ → «Не выявлено», «возможно» или «передано специалисту».
- ☐ Проведена первичная Article 6 проверка
- ☐ → Annex I, Annex III, Article 6(3), profiling и дата применимости.
- ☐ Определены меры AI-грамотности
- ☐ → Кто использует систему, что должен знать и как поддерживается компетентность.
- ☐ Проверен Article 50
- ☐ → Кто и что обязан сообщать, маркировать или раскрывать.
- ☐ Проверены данные, DPIA и FRIA
- ☐ → Статус каждой отдельной проверки и ответственный специалист.
- ☐ Создан реестр действий
- ☐ → Действие, владелец, срок, доказательство выполнения, дата следующего пересмотра.

Метод

- ☐ Проверяйте один сценарий за раз.
- ☐ Неизвестный ответ означает «требуется проверка».
- ☐ Роль организации может меняться между сценариями.
- ☐ Обязанность закона, официальное разъяснение и полезная практика — разные уровни.
- ☐ Первичная проверка не заменяет юридическую квалификацию.

Обозначения

- ☐ **ДЕЙСТВУЮЩАЯ НОРМА** — обязательное правило, применимое на дату cutoff.
- ☐ **БУДУЩЕЕ ОБЯЗАТЕЛЬСТВО** — правило с будущей датой применения.
- ☐ **ОФИЦИАЛЬНОЕ РАЗЪЯСНЕНИЕ** — guidance органа ЕС, не равное закону.
- ☐ **РАБОЧАЯ ПРАКТИКА** — полезная организационная мера, не представленная как обязательная.
- ☐ **ТРЕБУЕТ ПРОВЕРКИ** — недостаточно фактов или нужна профессиональная квалификация.

Ключевые даты AI Act

Не начинайте проверку с календаря. Сначала выберите маршрут и только затем смотрите даты, относящиеся к вашему сценарию.

СЕЙЧАС

1 августа 2024 AI Act вступил в силу.

2 февраля 2025 Применяются определения, Article 4 и восемь первоначальных категорий запрещённых практик Article 5.

2 августа 2025 Начали применяться правила для новых GPAI-моделей, отдельные положения governance и национальная рамка санкций.

27 июля 2026 Вступил в силу Regulation (EU) 2026/1744.

2 августа 2026 Начал применяться Article 50; применяется основная оставшаяся часть регулирования и enforcement для GPAI.

БЛИЖАЙШИЕ ИЗМЕНЕНИЯ

2 декабря 2026 Начинаят применяться две новые категории Article 5. Истекает ограниченный переходный срок Article 50(2) для определённых систем, ранее выведенных на рынок.

2 августа 2027 Завершается переходный период для GPAI-моделей, выведенных на рынок до 2 августа 2025. Государства должны обеспечить как минимум одну национальную regulatory sandbox.

ПОЗЖЕ

2 декабря 2027 Начинаят применяться правила high-risk для систем по Article 6(2) и Annex III.

2 августа 2028 Начинаят применяться правила high-risk для систем по Article 6(1) и Annex I.

Источники: S1 — Article 113; S2; S3.

Определите роль до проверки обязанностей

Название продукта не определяет вашу роль. Смотрите, кто создаёт, выводит на рынок, вводит в эксплуатацию и использует систему.

Организация, использующая систему под своей ответственностью — **deployer**

Использует AI-систему под своей властью и в рамках профессиональной деятельности.

Частая ошибка: считать deployer просто «конечным пользователем». Сотрудник может работать с инструментом, но юридическая роль обычно относится к организации.

Поставщик AI-системы — **provider**

Разрабатывает AI-систему или организует её разработку и выводит систему на рынок либо вводит в эксплуатацию под своим именем или товарным знаком.

Частая ошибка: считать provider только разработчика исходной модели.

Импортёр — **importer**

Находится в ЕС и выводит на рынок ЕС AI-систему, которая носит имя или товарный знак организации из третьей страны.

Частая ошибка: не проверить роль европейского участника договорной цепочки.

Дистрибьютор — **distributor**

Предоставляет AI-систему на рынке ЕС, не являясь provider или importer.

Частая ошибка: считать перепродажу или распространение юридически нейтральным.

Уполномоченный представитель — **authorised representative**

Находится в ЕС и по письменному мандату выполняет определённые задачи от имени provider из третьей страны.

Частая ошибка: путать эту роль с обычным консультантом или торговым представителем.

Поставщик GPAI-модели — **GPAI provider**

Разрабатывает или организует разработку модели AI общего назначения и выводит её на рынок.

Частая ошибка: считать любую компанию, использующую API или создающую оболочку над моделью, поставщиком GPAI-модели.

Article 25 — когда роль может измениться

Если вы ставите своё имя или товарный знак на high-risk систему, существенно её изменяете либо меняете назначение так, что система становится high-risk, обязанности provider могут перейти к вам.

Это не автоматический вывод для любого изменения. Зафиксируйте факты и проведите отдельную оценку Article 25.

Ключевые термины

- ☐ Вывод на рынок — **placing on the market**: первое предоставление продукта на рынке ЕС.
- ☐ Ввод в эксплуатацию — **putting into service**: первое предоставление для использования непосредственно deployer или для собственного использования в ЕС.
- ☐ Результат системы — **output**: созданный системой прогноз, рекомендация, решение, контент или иной результат.
- ☐ **Human oversight**: содержательный человеческий контроль с полномочиями вмешаться.
- ☐ **GPAI**: модель AI общего назначения, способная выполнять широкий круг задач.

Источники: S1 — Articles 3 и 25.

Есть ли сигнал, при котором использование нужно остановить?

ОСТАНОВИТЬ → ПРОВЕРИТЬ → ПЕРЕДАТЬ СПЕЦИАЛИСТУ

Не пытайтесь самостоятельно окончательно квалифицировать пограничный случай. Если функция может относиться к Article 5, не запускайте её до проверки.

ДЕЙСТВУЕТ СЕЙЧАС

ДЕЙСТВУЮЩАЯ НОРМА

Проверьте восемь первоначальных категорий:

1. Манипулятивные или скрытые техники, способные существенно исказить поведение и причинить значительный вред.
2. Использование уязвимости, связанной с возрастом, инвалидностью либо социальным или экономическим положением, с риском значительного вреда.
3. Социальная оценка людей, приводящая к неблагоприятному обращению в несвязанном контексте либо к неоправданному или несоразмерному обращению.
4. Оценка или прогноз риска совершения преступления только на основе profiling или личностных характеристик, кроме предусмотренной законом поддержки человеческой оценки на основе объективных и проверяемых фактов.
5. Создание или расширение баз распознавания лиц посредством неизбирательного сбора изображений из интернета или камер наблюдения.
6. Вывод об эмоциях в рабочей или образовательной среде, кроме ограниченных медицинских или связанных с безопасностью случаев.
7. Биометрическая категоризация для вывода определённых чувствительных или защищённых характеристик, с предусмотренными законом ограниченными исключениями.
8. Удалённая биометрическая идентификация в реальном времени в публичных местах для правоохранных целей, кроме строго ограниченных и разрешённых случаев.

БУДЕТ ДЕЙСТВОВАТЬ С 2 ДЕКАБРЯ 2026

БУДУЩАЯ НОРМА

В установленных Regulation (EU) 2026/1744 случаях добавляются две категории:

генерация или манипулирование реалистичным материалом, относящимся к интимным частям тела или сексуально откровенным действиям идентифицируемого человека без предусмотренного нормой свободного, конкретного, информированного, недвусмысленного и явного согласия; генерация или манипулирование материалом сексуального насилия над детьми без законного основания.

Норма различает вывод на рынок, ввод в эксплуатацию и использование, а также учитывает предусмотренные safeguards и границы, описанные в recitals.

Что зафиксировать

- ☐ какая функция вызывает вопрос;
- ☐ кто её предоставляет и использует;
- ☐ какие люди и данные затронуты;
- ☐ где и для какой цели применяется результат;
- ☐ приостановлена ли функция;
- ☐ кому передан вопрос.

Результат checklist не является юридическим разрешением продолжить использование.

Источники: S1 — Article 5; S2; S3; S4.

Нужна ли этому сценарию high-risk проверка?

Проверка high-risk не начинается с общего впечатления о том, что система «важная» или «опасная». Нужны назначение, категория и роль.

1. Annex I (Приложение I)

БУДУЩАЯ НОРМА

Проверьте, является ли AI-система компонентом безопасности продукта или самостоятельным продуктом, регулируемым законодательством из Annex I, и требуется ли для такого продукта независимая оценка соответствия третьей стороной.

Примеры могут включать отдельные регулируемые медицинские, машинные и другие продуктовые режимы. Наличие AI в продукте само по себе ещё не завершает тест.

Дата применения соответствующей high-risk ветки: 2 августа 2028.

2. Annex III (Приложение III)

БУДУЩАЯ НОРМА

Проверьте назначение системы в перечисленных областях:

биометрия;
критическая инфраструктура;
образование и профессиональная подготовка;
трудоустройство и управление работниками;
доступ к существенным частным и публичным услугам;
правоохранительная деятельность;
миграция, убежище и пограничный контроль;
правосудие и демократические процессы.

Дата применения соответствующей high-risk ветки: 2 декабря 2027.

3. Article 6(3)

Для отдельных систем из Annex III предусмотрена ограниченная возможность обосновать, что система не создаёт существенного риска для здоровья, безопасности или основных прав и существенно не влияет на результат принятия решения.

Не используйте Article 6(3) как общее исключение. Нужны факты, документирование и проверка предусмотренных нормой условий.

4. Profiling

БУДУЩАЯ НОРМА

Если система выполняет profiling физических лиц в предусмотренном Annex III контексте, не считайте её автоматически исключённой по Article 6(3). Этот фактор требует отдельной квалификации.

Рабочий результат

Выберите один статус:

- ☐ признаков Annex I/III не выявлено;
- ☐ возможна high-risk категория;
- ☐ нужна проверка Article 6(3);
- ☐ profiling требует отдельной оценки;
- ☐ передано legal/compliance.

До дат применения используйте результат для подготовки, а не для утверждения, что все будущие обязанности уже действуют.

Источники: S1 — Articles 6 и 113; S2; S3; S11 — draft/non-binding на cutoff.

Использую ChatGPT, Claude или Gemini. Что сделать сейчас?

- ☐ Обычное использование готового AI-сервиса не освобождает от проверки, но и не делает организацию автоматически provider модели или high-risk оператором.

ПО ЗАКОНУ: ПРОВЕРЬТЕ ПРИМЕНИМОСТЬ

- ☐ 1. Определите роль. Обычно организация является deployer используемой системы, но интеграция, ребрендинг и изменение назначения могут изменить вывод.
- ☐ 2. Проверьте Article 4. Нужны меры, поддерживающие AI-грамотность людей, работающих с системой.
- ☐ 3. Проверьте Article 50. Особенно для чат-интерфейса, публичного AI-контента, deepfake и чувствительных функций.
- ☐ 4. Исключите сигналы Article 5 и Article 6.
- ☐ 5. Проверьте GDPR и отраслевые правила. Особенно при персональных, чувствительных или конфиденциальных данных.

Минимальная карточка сценария

ПОЛЕ	ЧТО ЗАПИСАТЬ
Инструмент	Название и версия, если известна
Сценарий	Конкретная рабочая задача
Кто использует	Команда или функции
Данные	Какие данные вводятся и откуда
Результат	Где используется output
Проверка человеком	Кто проверяет и что может изменить
Эскалация	К кому обратиться при сомнении
Пересмотр	Дата следующей проверки

- ☐ Не записывайте «соответствует AI Act». Записывайте проверенные факты, решения и оставшиеся вопросы.

ОРГАНИЗИРУЙТЕ РАБОТУ

- ☐ Ведите список используемых AI-инструментов и сценариев.
- ☐ Назначьте владельца каждого сценария.
- ☐ Зафиксируйте разрешённые и запрещённые данные.
- ☐ Сохраните условия и документацию поставщика.
- ☐ Определите, какой результат требует человеческой проверки.
- ☐ Установите путь эскалации для ошибки, вреда или сомнения.
- ☐ Периодически пересматривайте сценарий и настройки.

AI-грамотность: что действительно требует закон?

В этой checklist под AI-грамотностью (AI literacy) мы понимаем навыки, знания и понимание, которые помогают осознанно использовать AI-системы и видеть их возможности, риски и возможный вред с учётом роли и обязанностей.

ДЕЙСТВУЮЩАЯ НОРМА

Provider и deployer должны принимать меры, поддерживающие AI-грамотность сотрудников и других лиц, работающих с AI-системами от их имени. При выборе мер учитываются знания, опыт, образование, подготовка, контекст использования и затрагиваемые люди или группы.

Закон не устанавливает автоматически

- ☐ единый курс для всех;
- ☐ обязательное количество часов;
- ☐ универсальный сертификат;
- ☐ гарантированный числовой уровень знаний;
- ☐ отдельную должность AI officer;
- ☐ обязательного DPO только из-за использования AI;
- ☐ отдельный AI governance board для каждой организации.

Полезные меры — примеры, а не универсальные обязательства

- ☐ короткий вводный модуль для всех пользователей;
- ☐ отдельное обучение для владельца чувствительного процесса;
- ☐ правила работы с персональными и конфиденциальными данными;
- ☐ разбор типичных ошибок и ограничений системы;
- ☐ инструкция по человеческой проверке;
- ☐ канал сообщения об ошибках и инцидентах;
- ☐ повторная проверка знаний после изменения инструмента или сценария.

Что сохранить

- ☐ кому требовалась подготовка;
- ☐ почему выбран такой уровень;
- ☐ какие материалы использованы;
- ☐ когда мера проведена;
- ☐ когда её нужно пересмотреть.

Не обещайте «полное знание AI». Покажите, что меры соответствуют роли, контексту и риску.

Источники: S1 — Article 4; S2; S5.

С кем взаимодействует система и какой контент создаёт?

Article 50 распределяет обязанности между разными участниками. Не существует одной универсальной маркировки для любого AI-контента.

Поставщик: прямое взаимодействие с человеком

ДЕЙСТВУЮЩАЯ НОРМА

Provider системы, предназначенной для непосредственного взаимодействия с людьми, должен спроектировать её так, чтобы человек был информирован о взаимодействии с AI, если это не очевидно для разумно информированного, внимательного и осмотрительного человека.

Поставщик: синтетический контент

ДЕЙСТВУЮЩАЯ НОРМА

Provider системы, создающей синтетические аудио, изображения, видео или текст, должен обеспечить маркировку output в машиночитаемом формате и возможность обнаружить, что результат был создан или изменён AI, с учётом предусмотренных нормой технических условий и исключений.

Организация-deployer: распознавание эмоций или биометрическая категоризация

ДЕЙСТВУЮЩАЯ НОРМА

Deployer должен информировать затронутых людей об использовании соответствующей системы. Обработка персональных данных отдельно проверяется по GDPR.

Организация-deployer: deepfake

ДЕЙСТВУЮЩАЯ НОРМА

Deployer, использующий систему для создания или изменения deepfake, должен раскрывать искусственный характер контента в соответствии с Article 50.

Организация-deployer: текст по вопросам общественного интереса

ДЕЙСТВУЮЩАЯ НОРМА

При публикации AI-сгенерированного или изменённого текста для информирования общественности по вопросам общественного интереса проверяется обязанность раскрытия.

Предусмотренное нормой исключение может применяться, если контент прошёл человеческую проверку или редакционный контроль и физическое или юридическое лицо несёт редакционную ответственность. Это не общее исключение для любого отредактированного текста.

Переход Article 50(2)

ДЕЙСТВУЮЩАЯ НОРМА

Для определённых provider систем, выведенных на рынок до 2 августа 2026, переход по Article 50(2) действует до 2 декабря 2026.

Это не перенос всего Article 50.

Рабочий результат

Запишите:

- ☐ какой тип взаимодействия или контента рассматривается;
- ☐ кто является обязанным участником;
- ☐ какое раскрытие или техническая маркировка проверены;
- ☐ какое исключение предполагается и на каких фактах;
- ☐ какая документация поставщика подтверждает вывод.

Источники: S1 — Article 50; S2; S3; S9; S10.

Читайте этот раздел только тогда, когда маршрут привёл вас к high-risk проверке

Не переносите эти обязанности автоматически на обычное использование AI.

Даты

БУДУЩАЯ НОРМА

Annex III / Article 6(2): 2 декабря 2027
Annex I / Article 6(1): 2 августа 2028

Если вы provider high-risk системы

БУДУЩАЯ НОРМА

Проверьте применимые требования к:

системе управления рисками;
данным и data governance;
технической документации;
журналированию;
информации и инструкциям для deployer;
проектированию human oversight;
точности, устойчивости и кибербезопасности;
системе качества;
оценке соответствия и регистрации.

Если вы deployer high-risk системы

БУДУЩАЯ НОРМА

Проверьте применимые требования к:

использованию по инструкциям provider;
компетентным и уполномоченным людям для human oversight;
качеству и релевантности входных данных, когда они находятся под вашим контролем;
мониторингу работы;
хранению доступных журналов;
сообщениям об инцидентах;
информированию затронутых работников и людей, когда это требуется;
DPIA и FRIA, если соответствующие тесты применимы;
регистрации и другим отраслевым требованиям.

Article 14 и Article 26 — не одно и то же

Article 14 требует от provider спроектировать high-risk систему так, чтобы был возможен эффективный человеческий контроль.

Article 26 устанавливает обязанности deployer при эксплуатации high-risk системы.

Ни одна из норм не создаёт одну универсальную письменную процедуру для любого использования AI.

Что можно сделать заранее

- ☐ уточнить intended purpose;
- ☐ собрать инструкции и технические материалы;
- ☐ распределить роли;
- ☐ определить будущий контроль;
- ☐ проверить данные и logging;
- ☐ составить план готовности к соответствующей дате.

Источник: S1 — Articles 8–27; S2; S3.

Пользуюсь API, собираю решение или поставляю продукт?

ПОЛЬЗУЮСЬ API

Вы вызываете внешнюю модель внутри своего процесса, но не выводите модель на рынок под своим именем.

Обычно это не делает вас GPAI provider. Проверьте роль deployer, конкретный сценарий, Article 4, Article 50, GDPR и договорные ограничения.

СОБИРАЮ РЕШЕНИЕ НА ЧУЖИХ МОДЕЛЯХ

Вы создаёте интерфейс, автоматизацию или решение-оболочку (wrapper) на базе внешней модели.

ДЕЙСТВУЮЩАЯ НОРМА

Это не делает вас автоматически поставщиком исходной GPAI-модели. Но вы можете стать provider AI-системы, которую выводите на рынок или вводите в эксплуатацию под своим именем.

Зафиксируйте, кто отвечает за модель, систему, интерфейс, данные, документацию и итоговое назначение.

ПОСТАВЛЯЮ AI-СИСТЕМУ

Вы разрабатываете или организуете разработку системы и выводите её на рынок либо вводите в эксплуатацию под своим именем или товарным знаком.

Проверьте:

- ☐ intended purpose;
- ☐ территориальную связь;
- ☐ Article 5 и Article 6;
- ☐ Article 50;
- ☐ документацию и инструкции;
- ☐ цепочку поставки;
- ☐ изменение роли по Article 25.

ПОСТАВЛЯЮ GPAI-МОДЕЛЬ

ДЕЙСТВУЮЩАЯ НОРМА

Вы разрабатываете или организуете разработку модели общего назначения и выводите её на рынок.

Article 53 включает требования к технической документации, информации для downstream provider, политике соблюдения авторского права, публичному summary содержания обучения по официальному template и уполномоченному представителю, когда он требуется.

Для GPAI-модели с системным риском Article 55 добавляет оценку модели и adversarial testing, оценку и снижение системных рисков, incident reporting и кибербезопасность. Объём вычислений, использованный для обучения модели, свыше 10^{25} FLOPs создаёт презумпцию high-impact capabilities. Классификация учитывает процедуру Article 52; кроме того, Комиссия может квалифицировать модель как GPAI с системным риском по Article 51(1)(b).

Article 25 — сигналы изменения роли

БУДУЩАЯ НОРМА

Передайте вопрос на отдельную оценку, если вы:

размещаете своё имя или товарный знак на high-risk системе;
существенно изменяете high-risk систему;
меняете назначение системы так, что она становится high-risk.

GPAI: даты

ДЕЙСТВУЮЩАЯ НОРМА

2 августа 2025: правила для новых GPAI-моделей.
2 августа 2026: enforcement.
2 августа 2027: окончание перехода для моделей, выведенных на рынок до 2 августа 2025.

Кодекс GPAI является добровольным инструментом, официально признанным подходящим механизмом поддержки выполнения соответствующих обязанностей.

Источники: S1 — Articles 25, 51, 53 и 55; S3; S6–S8; S14.

Три разных вопроса о данных и правах

GDPR — Общий регламент ЕС по защите данных

Когда проверять: когда система обрабатывает персональные данные.

Что проверяет: правовое основание, цели, минимизацию данных, прозрачность, безопасность, права людей и сроки хранения.

Чего не означает: использование AI не отменяет GDPR и не делает любую обработку автоматически незаконной.

Кому передать: DPO, privacy/legal или ответственному за защиту данных.

DPIA — оценка воздействия на защиту данных

Когда проверять: когда обработка может создавать высокий риск для прав и свобод людей по Article 35 GDPR.

Что проверяет: необходимость и соразмерность обработки, риски для данных и меры их снижения.

Чего не означает: DPIA не требуется автоматически для каждого AI-инструмента.

Для применимого high-risk сценария Article 26(9) требует использовать предоставленную provider информацию при проведении DPIA.

Кому передать: DPO/privacy/legal с участием владельца процесса и технической команды.

FRIA — оценка воздействия на основные права

Будущая норма

Когда проверять: для определённых deployer и сценариев Article 27, включая публично-правовые организации, частных поставщиков публичных услуг и отдельные Annex III случаи в кредитовании и страховании жизни или здоровья.

Что проверяет: воздействие конкретного high-risk использования на основные права и предусмотренные меры.

Чего не означает: FRIA не является универсальной оценкой для любого AI-проекта.

Для ветки Annex III соответствующие high-risk правила начинают применяться 2 декабря 2027.

Кому передать: legal/compliance, владельцу процесса и специалистам по основным правам.

Координация, а не замена

Будущая норма

FRIA может использовать или ссылаться на части работы, уже выполненной в DPIA. Одна оценка не отменяет автоматически другую.

Рабочий результат

ПРОВЕРКА	СТАТУС
GDPR	применим / не выявлен триггер / требуется проверка
DPIA	требуется / не требуется по текущим фактам / передано DPO
FRIA	возможна / не выявлен score / передано legal
AI Act	отдельный статус Article 5, 6, 26 и 27

Источники: S1 — Articles 26(9) и 27; S2; S13 — Article 35.

Малый бизнес не освобождён, но пропорциональность учитывается

Микро-, малые и средние предприятия — МСП (SME) — не получают общего освобождения от AI Act.

Меры поддержки

- ☐ приоритетный доступ к regulatory sandbox и поддержка экспериментов;
- ☐ информационные и обучающие инициативы, адаптированные к потребностям МСП;
- ☐ специальные каналы связи с компетентными органами;
- ☐ поддержка участия в стандартизации;
- ☐ сниженные и пропорциональные сборы за оценку соответствия;
- ☐ учёт размера и экономических возможностей при применении мер и санкций.

Максимальные пределы административных штрафов

НАРУШЕНИЕ	МАКСИМАЛЬНЫЙ ПРЕДЕЛ
Article 5	€35 млн или 7%
Другие перечисленные обязанности	€15 млн или 3%
Неточная, неполная или вводящая в заблуждение информация	€7,5 млн или 1%
Обязанности GPAI provider	€15 млн или 3%

Важное различие Articles 99 и 101

ДЕЙСТВУЮЩАЯ НОРМА Для МСП Article 99(6) применяет меньший из абсолютного и процентного пределов к санкциям, предусмотренным Article 99(3)–(5).
Article 101 устанавливает отдельный максимум для GPAI provider: €15 млн или 3% мирового годового оборота — в зависимости от того, что выше.
Формулу Article 101 нельзя автоматически заменять правилом Article 99(6).
Максимальный предел не является обычным результатом любой ошибки. Учитываются характер, тяжесть, длительность, умысел, последствия и другие обстоятельства.
Практический вывод: небольшой размер бизнеса важен для пропорциональности, но не заменяет проверку применимых обязанностей.
Источники: S1 — Articles 62, 99 и 101; S2; S14.

Как пользоваться маршрутами

ПРИМЕЧАНИЕ

01 / Малый бизнес в Италии использует ChatGPT для маркетинга

Ситуация — команда готовит черновики постов и писем, затем сотрудник проверяет и публикует текст. Территориальный статус — связь с ЕС подтверждена. Маршрут — А.

Проверить — роль deployer, Article 4, публичный контент по Article 50, персональные и конфиденциальные данные.

Сделать — создать карточку сценария, правила данных, человеческую проверку и критерии публикации.

Запросить у поставщика — условия использования, privacy и материалы о прозрачности.

Передать специалисту — использование персональных данных, sensitive campaigns, спорные права на контент.

Этот кейс не доказывает — что весь маркетинговый AI-контент требует одной и той же маркировки или что бизнес полностью соответствует AI Act.

02 / AI помогает отбирать кандидатов в ЕС

Ситуация — система ранжирует резюме и рекомендует, кого пригласить на интервью.

Территориальный статус — связь с ЕС подтверждена.

Маршрут — В; возможно С, если компания предоставляет решение.

Проверить — Article 5, Annex III employment, profiling, GDPR, DPIA и будущие high-risk обязанности.

Сделать — описать влияние системы на решение, данные, критерии, человеческий контроль и механизм оспаривания.

Запросить у поставщика — intended purpose, ограничения, характеристики качества, документацию, logging и инструкции по oversight.

Передать специалисту — high-risk квалификацию, трудовое право, дискриминационные риски, DPIA.

Этот кейс не доказывает — что человеческое подтверждение автоматически исключает high-risk или устраняет риск для прав кандидата.

03 / Компания создаёт своё AI-решение

Ситуация — компания соединяет стороннюю модель, собственные данные и интерфейс, затем продаёт решение клиентам.

Территориальный статус — зависит от учреждения, рынка, ввода в эксплуатацию, результата и цепочки поставки.

Маршрут — С; при работе из третьей страны также D.

Проверить — provider системы, GPAI provider исходной модели, Article 25, Article 50, Article 5/6 и договорную цепочку.

Сделать — разделить модель, систему, интерфейс и процесс; составить карту ролей и ответственности.

Запросить у поставщика модели — технические материалы, ограничения, правила использования, информацию для downstream provider.

Передать специалисту — квалификацию продукта, договоры, территориальный scope, high-risk и ответственность.

Этот кейс не доказывает — что использование API делает компанию GPAI provider или, наоборот, освобождает её от роли provider собственной системы.

Публичный контент, рынок ЕС и язык

ПРИМЕЧАНИЕ

04 / Публичный AI-generated content

Ситуация — организация публикует созданные AI изображения, видео, аудио или текст.

Территориальный статус — определяется отдельно.

Маршрут — А или С; страница 11 обязательна для проверки.

Проверить — кто создаёт и публикует контент, его тип, public-interest context, deepfake, техническую маркировку и редакционную ответственность.

Сделать — зафиксировать workflow публикации и человеческий контроль.

Запросить у поставщика — сведения о машиночитаемой маркировке и обнаружимости AI-output.

Передать специалисту — deepfake, sensitive content, исключения, авторское право и права личности.

Этот кейс не доказывает — что любой AI-текст обязан иметь одинаковую видимую надпись.

05 / Компания вне ЕС работает с европейским рынком

Ситуация — компания находится вне ЕС и предоставляет AI SaaS европейским организациям.

Территориальный статус — возможна применимость; нужны факты.

Маршрут — D + C; В при чувствительном назначении.

Проверить — вывод системы на рынок ЕС, ввод в эксплуатацию, intended purpose, использование output в ЕС и цепочку импортёров, дистрибьюторов или представителей.

Сделать — подготовить территориальную записку по продукту, договорам, рынку и фактическому использованию.

Запросить у партнёров — роли, место поставки и эксплуатации, предполагаемое использование результата.

Передать специалисту — Article 2, представитель в ЕС, договоры и продуктовую квалификацию.

Этот кейс не доказывает — что наличие европейского клиента автоматически делает AI Act применимым.

06 / Русскоязычный предприниматель работает в Италии или другой стране ЕС

Ситуация — владелец и команда говорят по-русски, но компания учреждена в ЕС и использует AI в европейском бизнес-процессе.

Территориальный статус — связь с ЕС подтверждена.

Маршрут — А, В или С в зависимости от деятельности.

Маршрут D не выбирается только из-за русского языка.

Проверить — конкретную роль, назначение, данные, людей, output и национальный слой соответствующей страны.

Сделать — вести документацию на рабочем языке команды, сохраняя точные legal terms и официальные документы.

Передать специалисту — вопросы AI Act, GDPR и права той страны, с которой связан сценарий.

Этот кейс не доказывает — что к организации применимо российское право или что страна определяется языком документа.

Проверьте правила страны, с которой связан ваш сценарий

AI Act создаёт общий уровень ЕС, но рядом могут действовать:

- ☐ национальные законы об AI;
- ☐ компетентные и надзорные органы;
- ☐ отраслевые правила;
- ☐ законодательство о защите данных;
- ☐ трудовое, потребительское, медицинское, финансовое и иное право;
- ☐ решения судов и регуляторов.

Язык команды и гражданство владельца не выбирают национальный слой автоматически.

Запишите:

- ☐ 1. где учреждена организация;
- ☐ 2. где используется система;
- ☐ 3. где находятся затронутые люди;
- ☐ 4. на какой рынок поставляется продукт;
- ☐ 5. какой отраслевой режим действует;
- ☐ 6. какой национальный специалист нужен.

ПРИМЕЧАНИЕ

Если сценарий связан с конкретной страной, отдельно определите применимое национальное право, органы, отраслевые требования и правила защиты данных. Не выбирайте Россию или Италию автоматически.

Если есть связь с Италией

ДЕЙСТВУЮЩАЯ НОРМА

Legge 23 settembre 2025, n. 132 опубликована 25 сентября 2025 и вступила в силу 10 октября 2025. Её положения применяются вместе с Regulation (EU) 2024/1689.

Компетентные органы

ДЕЙСТВУЮЩАЯ НОРМА

AgID выполняет функции notifying authority в предусмотренной национальной рамке.

ACN выполняет функции market surveillance authority и единого контактного пункта.

Banca d'Italia, CONSOB и IVASS сохраняют компетенции в соответствующих регулируемых секторах.

Garante per la protezione dei dati personali сохраняет полномочия по защите персональных данных.

Другие отраслевые органы сохраняют предусмотренные законом компетенции.

Итальянский слой используется только при доказанной связи сценария с Италией. Он не становится национальным слоем RU edition автоматически.

Превратите проверку в конкретные действия

СДЕЛАЙТЕ ВНУТРИ КОМАНДЫ

- ☐ опишите один сценарий;
- ☐ зафиксируйте территориальные факты;
- ☐ определите рабочую гипотезу о роли;
- ☐ составьте карту данных и результата;
- ☐ назначьте владельца процесса;
- ☐ определите человеческую проверку;
- ☐ создайте реестр действий и пересмотра.

ЗАПРОСИТЕ У ПОСТАВЩИКА

- ☐ intended purpose и ограничения;
- ☐ инструкции по эксплуатации;
- ☐ информацию о данных и logging;
- ☐ сведения об Article 50 и маркировке output;
- ☐ документы для downstream provider;
- ☐ сведения о human oversight;
- ☐ информацию для DPIA и high-risk подготовки, если применимо;
- ☐ актуальные условия и сведения об изменениях системы.

АРХИТЕКТУРА ПРОЦЕССОВ И КОНТРОЛЯ — CRITERIO DIGITALE

Criterio Digitale может помочь:

- ☐ составить карту AI-сценариев;
- ☐ описать процесс и точки решений;
- ☐ разграничить рабочие роли;
- ☐ спроектировать контроль человека;
- ☐ организовать поток документации;
- ☐ связать риски, действия и ответственных;
- ☐ настроить traceability;
- ☐ подготовить вопросы для поставщика и специалиста.

Это работа с процессами, системой управления и документацией. Она не заменяет юридическую консультацию.

ЮРИДИЧЕСКАЯ ОЦЕНКА / DPO

Передайте специалисту:

- ☐ окончательную территориальную применимость;
- ☐ Article 5;
- ☐ high-risk юридическую классификацию;
- ☐ Article 25 и ответственность в цепочке поставки;
- ☐ DPIA и FRIA;
- ☐ договоры, ответственность и национальное право;
- ☐ спорные вопросы защиты данных и основных прав.

Минимальный итог

После checklist у вас должны быть:

- ☐ 1. карта сценария;
- ☐ 2. маршрут;
- ☐ 3. факты и документы;
- ☐ 4. перечень неизвестного;
- ☐ 5. план действий;
- ☐ 6. адресная передача вопросов специалистам.

Официальные источники S1–S6

S1	Regulation (EU) 2024/1689 European Parliament and Council / EUR-Lex Статус: обязательное право Публикация: 2024-07-12 Обновление: 2026-07-27 Вступление в силу: 2024-08-01 Проверено: 2026-09-01 Официальный источник ↗	S4	Guidelines on prohibited artificial intelligence practices European Commission Статус: официальный материал, не имеющий силы закона Публикация: 2025-02-04 Обновление: 2025-07-31 Проверено: 2026-09-01 Официальный источник ↗
S2	Regulation (EU) 2026/1744 European Parliament and Council / EUR-Lex Статус: обязательное право Публикация: 2026-07-24 Вступление в силу: 2026-07-27 Проверено: 2026-09-01 Официальный источник ↗	S5	AI Literacy — Questions & Answers European Commission / AI Office Статус: официальный материал, не имеющий силы закона Проверено: 2026-09-01 Официальный источник ↗
S3	Timeline for the Implementation of the EU AI Act European Commission - AI Act Service Desk Статус: официальный материал, не имеющий силы закона Проверено: 2026-09-01 Официальный источник ↗	S6	Guidelines for providers of general-purpose AI models European Commission Статус: официальный материал, не имеющий силы закона Публикация: 2025-07-18 Обновление: 2026-04-20 Проверено: 2026-09-01 Официальный источник ↗

Официальные источники S7–S14

ПРИМЕЧАНИЕ

Проект, template, добровольный кодекс или официальное разъяснение не заменяют обязательный текст Regulation и профессиональную оценку конкретного случая.

S7	General-Purpose AI Code of Practice European Commission / AI Office Статус: добровольный инструмент Публикация: 2025-07-10 Обновление: 2026-07-31 Проверено: 2026-09-01 Официальный источник ↗	S10	Code of Practice on Transparency of AI-generated Content European Commission / AI Office Статус: добровольный инструмент Публикация: 2026-06-10 Обновление: 2026-07-31 Проверено: 2026-09-01 Официальный источник ↗
S8	Template for the Public Summary of Training Content European Commission / AI Office Статус: официальный инструмент Публикация: 2025-07-24 Обновление: 2026-03-26 Проверено: 2026-09-01 Официальный источник ↗	S11	Guidelines for providers and deployers of high-risk AI systems European Commission Статус: проект, не имеющий силы закона Проверено: 2026-09-01 Официальный источник ↗
S9	Guidelines on transparency obligations under Article 50 European Commission Статус: официальный материал, не имеющий силы закона Публикация: 2026-07 Обновление: 2026-08-06 Проверено: 2026-09-01 Официальный источник ↗	S12	Legge 23 settembre 2025, n. 132 Repubblica Italiana / Normattiva Статус: обязательное право Публикация: 2025-09-25 Вступление в силу: 2025-10-10 Проверено: 2026-09-01 Официальный источник ↗
		S13	Regulation (EU) 2016/679 — General Data Protection Regulation (GDPR) European Parliament and Council / EUR-Lex Статус: обязательное право Публикация: 2016-05-04 Вступление в силу: 2016-05-24 Проверено: 2026-09-01 Официальный источник ↗
		S14	Commission Implementing Regulation (EU) 2026/1755 European Commission / EUR-Lex Статус: обязательное право Публикация: 2026-07-21 Проверено: 2026-09-01 Официальный источник ↗

О редакции

Версия: RU v1.0

Edition ID: RU-1.0 / EU-CORE / TERRITORIAL-ROUTES / ITALY-OPTIONAL

Legal/factual cutoff: 1 сентября 2026

Следующая плановая проверка: до 1 декабря 2026

Автор: Татьяна Мирошина

Проект: Criterio Digitale

Проверить раньше плановой даты, если:

- ☐ изменился AI Act или связанный имплементационный акт;
- ☐ опубликована финальная high-risk guidance;
- ☐ изменились официальные guidelines Article 4, 5 или 50;
- ☐ изменился продукт, назначение, рынок или роль организации;
- ☐ появился новый national layer;
- ☐ изменился используемый provider или модель;
- ☐ возник инцидент, жалоба или значительное воздействие на людей.

Границы документа

Checklist помогает:

- ☐ структурировать факты;
- ☐ выбрать рабочий маршрут;
- ☐ собрать документы;
- ☐ определить неизвестные вопросы;
- ☐ подготовить передачу специалисту.

Checklist не:

- ☐ определяет окончательную юридическую применимость;
- ☐ подтверждает соответствие;
- ☐ разрешает запрещённую или high-risk практику;
- ☐ заменяет DPIA, FRIA или юридическую консультацию;
- ☐ исследует национальное право всех возможных стран.

Используйте официальный текст закона и профессиональную оценку для конкретного случая.