РОЗДІЛ 4

Хто несе відповідальність — комплаєнс як організаційна архітектура

> *EU AI Act, GDPR і їхні американські відповідники перетворюють відповідальність на питання конструкції. Хто його ігнорує, той будує ризик, а не AI-систему.*

Цей розділ — регуляторна проекція розриву між машинною генерацією і людською верифікацією. EU AI Act, GDPR і їхні аналоги по інший бік Атлантики не усувають когнітивну асиметрію — вони фіксують її юридично. Розрив між тим, що генерує модель, і тим, що людина встигає перевірити, перекладається у мову прав і обов'язків: хто Provider (постачальник, який розробляє AI-систему або виводить її на ринок), хто Deployer (розгортач, який застосовує систему у власній діяльності), хто AI-оператор (людина, яка щодня веде систему в експлуатації), хто Compliance Officer (відповідальний за дотримання регуляторних вимог). Комплаєнс тут — юридичне виявлення тієї самої асиметрії.

EU AI Act набув чинності в серпні 2024 року. Перехідні періоди для більшості категорій високого ризику вже вийшли в активну фазу або входять у неї в найближчому горизонті після набуття чинності. Більшість виробників машинобудування у DACH-просторі ще не відчули його повної ваги. Коли перехідні періоди сплинуть, правила стануть обов'язковими, з санкціями до 30 мільйонів євро або 6% глобального річного обороту, залежно від того, що вище.

Питання *хто несе відповідальність* належить до конструкції, а не до юридичної післяобробки. У більшості проєктів його ставлять занадто пізно — у момент, коли архітектурне вікно вже зачинене. Цей розділ описує, як ставити це питання своєчасно — щоб відповідь на нього лишалася опорною.

Як до цього підходять в Європі та США

У США немає єдиного федерального аналога EU AI Act. Регулювання розпадається на три рівні: NIST AI Risk Management Framework (добровільний методичний стандарт), секторні норми (FTC щодо рекламних тверджень, FDA щодо медичного AI, EEOC щодо рекрутингу) і штатні закони (Colorado AI Act 2024, California SB 1047 і подібні). Загальна логіка — категоризація ризиків, документація, аудит, обов'язки розкриття — близька до європейської. Відмінності — швидкість набуття чинності, рівень санкцій і концентрація обов'язків на Deployer-і.

Далі в розділі доцільно детальніше розглянути тематику саме на європейському прикладі, оскільки європейський режим — суворіший. Хто будує комплаєнс під EU AI Act, той у переважній більшості випадків покриває і американські вимоги. Зворотний шлях — починати з менш суворого режиму і нарощувати при виході в EU — як правило, дорожчий, бо вимагає переробки архітектурних рішень, прийнятих без оглядки на EU-категорії ризику.

EU AI Act у практиці: класифікація високого ризику, документаційні обов'язки, відповідальні особи

Регулюючий текст називає конкретний перелік. Для індустріального DACH-контексту найбільш релевантні три категорії.

Безпека продукції. AI-системи, які є компонентами безпеки продуктів, що вже регулюються чинними EU-режимами — Maschinenrichtlinie (Регламент щодо машин і обладнання, 2023/1230), Medizinprodukteverordnung (Регламент про медичні вироби, MDR), Aviation Safety Regulation (Регламент безпеки авіації). Якщо AI-система якимось чином впливає на безпеку кінцевого продукту, з високою ймовірністю вона належить до високого ризику.

Критична інфраструктура. AI-системи для управління водопостачанням, енергетикою, транспортом. Для індустріальних виробників, які є частиною критичної інфраструктури, це означає додаткові вимоги.

Зайнятість і управління персоналом. Системи рекрутингу, оцінки продуктивності, розподілу завдань або моніторингу. Кожна AI-система, яка впливає на рішення стосовно співробітників, повинна перевірятися ретельно.

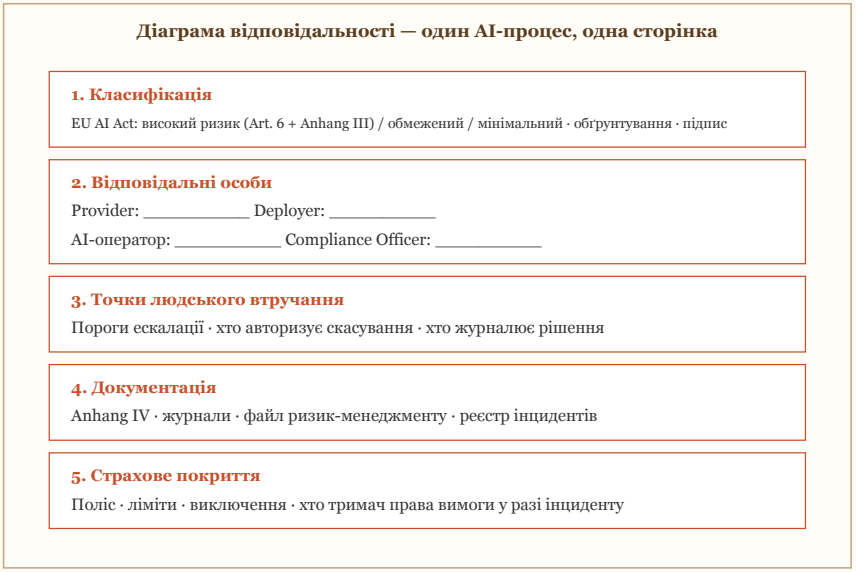
Для систем високого ризику EU AI Act вимагає: систему ризик-менеджменту до розгортання, управління якістю даних для тренувальних наборів, технічну документацію згідно з Anhang IV (Додаток IV), автоматичне журналювання, прозорість для кінцевих користувачів, людський нагляд (саме тут починає працювати 30%-шар), точність, стійкість і кібербезпеку.

І критично для нашого контексту: чітке визначення *Provider* і *Deployer*. Provider розробляє систему або виводить її на ринок. Deployer її розгортає. Обидва несуть обов'язки. Між ними може існувати договірне розподілення відповідальності — регулятор дивиться на обидва боки.

Стюарт Расселл у праці *Human Compatible* формулює загальне правило: відповідальність за автономну систему мусить мати інституційного носія до того, як система виходить на ринок. Кейт Кроуфорд у праці *Atlas of AI* додає, що цей носій ніколи не є *лише* технічною роллю

— він завжди вписаний у регуляторну, контрактну і організаційну архітектуру. EU AI Act у цій рамці узаконює вже існуючу вимогу: між моделлю і ринком має стояти названа особа з мандатом.

Діаграма відповідальності: п'ять питань для кожного AI-процесу



Структура діаграми відповідальності для одного AI-процесу (одне робоче навантаження, один продуктовий потік). Порядок заповнення: (1) класифікація за EU AI Act — на момент завершення пілота, перед рішенням про промислову експлуатацію; (2) відповідальні особи — на стадії планування, до старту розробки; (3) точки людського втручання — на стадії проектування, до тренування і інтеграції; (4) документація — формується поступово, фіналізується до запуску; (5) страхове покриття — до запуску. Кожен незаповнений блок працює як прихований ризик. Семантично діаграма повторює логіку трикутника

трьох ролей з Розділу 1: відповідальність структурно існує тоді, коли всі вершини мають названих носіїв з виписаним мандатом. Порожня вершина — це не нейтральна порожнеча, а структурна деформація, яка проявиться у момент інциденту. Адаптовано з матеріалів EU AI Act Implementation Toolkit (European Commission, Joint Research Centre, 2024) і RACI-схем ISO/IEC 42001 (AI Management System Standard, 2023).

Розподіл відповідальності за модулями: хто підписує що, коли, з якою страховкою

У реальних проєктах відповідальність рідко монолітна. Типова AI-система складається з кількох компонентів, кожен з власним ланцюжком відповідальності.

Модель. Хто Provider? Якщо модель куплена — постачальник. Якщо натренована самостійно — ви самі. Якщо це fine-tuned (донавчена, покращена під ваш контекст) стороння модель — відповідальність розділена, і деталі залежать від ліцензійного контракту.

Інфраструктура. Де живе модель? On-premises — ваша відповідальність за доступність і безпеку. Cloud (хмарна інфраструктура) — спільна відповідальність, але Deployer-обов'язок за EU AI Act цим не зменшується.

Інтеграція. Хто інтегрував модель у продакшн-середовище? Зовнішній інтегратор? Власна IT? Яка інтеграційна документація існує?

Експлуатація. Хто щодня веде систему? Це AI-оператор — і він має бути названий поіменно у комплаєнс-документації.

Практичний інструмент: матриця відповідальності по модулях, RACI-варіація (Responsible — виконавець, Accountable — відповідальний за результат, Consulted — консультант, Informed — інформований) для AI. Кожен рядок документує для одного модуля: хто Responsible, хто Accountable, хто підписант, яке страхове покриття. Це не бюрократична самоціль. Матриця дає відповідь на питання *хто підписує* в той момент, коли щось пішло не так. Щось завжди йде не так.

RACI-матриця для AI-системи: один рядок на модуль

Модуль	R	A	C	I	Страхування
Модель	Data-Team	CTO	Compliance	CEO	Cyber + E&O
Дані (training)	Data-Curator	DPO	Legal	CTO	GDPR-Liability
Інфраструктура	IT-Ops	CTO	CISO	CFO	Cyber-Polis
Інтеграція	Integrator	Head of IT	QA	CTO	Vendor-SLA
Експлуатація	AI-оператор	Process-Owner	Compliance	CEO	D&O + E&O

R — виконавець · A — відповідальний за результат (один на рядок) · C — консультант · I — інформований

Приклад заповненої RACI-матриці для типової AI-системи високого ризику в індустріальному DACH-контексті. Кожен модуль (рядок) має рівно одного Accountable; решта ролей розподіляється за фактичною компетенцією. Колонка «Страхування» називає тип поліса, який покриває інциденти у відповідному модулі: Cyber + E&O (errors-and-omissions), GDPR-Liability, D&O (directors-and-officers), Vendor-SLA. Порожнє поле — структурний дефект. Стандарт ISO/IEC 42001 (AI Management System Standard, 2023) розширює класичну RACI обов'язком документувати імена носіїв ролі, не лише посади.

Удавана суверенність (Sovereign-Washing): чому «EU-Cloud» рідко означає звільнення від відповідальності

Удавана суверенність (Sovereign-Washing) — маркетингова практика, яка стає поширенішою у DACH-просторі. Cloud-провайдери рекламують *DSGVO-сумісну (Datenschutz-Grundverordnung — європейський загальний регламент про захист даних, у міжнародному ужитку GDPR) EU-Cloud* або *sovereign AI* і натякають, що ці маркетингові позначки знімають з клієнта відповідальність за результати системи.

Вони цього не роблять.

Deployer-обов'язок за EU AI Act не залежить від місцезнаходження. Хто є Deployer-ом AI-системи високого ризику, несе Deployer-обов'язки — байдуже, у датацентрі в Мюнхені, Парижі чи Дубліні. *EU-Cloud* означає, що дані зберігаються в межах EU. Це може полегшити GDPR-комплаєнс при передаванні даних. Це нічого не змінює стосовно того, хто відповідає за результати системи.

GDPR-договір про обробку даних — Auftragsverarbeitungsvertrag (договір про обробку персональних даних на замовлення, у міжнародному ужитку Data Processing Agreement, DPA), скорочено AVV — з Cloud-провайдером робить його Auftragsverarbeiter (обробник за дорученням), який діє за вашими інструкціями. Якщо щось пішло не так, регулятор спочатку звертається до вас як до Verantwortlicher (контролер даних). Право вимоги відшкодування з провайдера (регрес) можливо існує — але це ваша проблема, не проблема регулятора.

Окремий ризик — доступність. *EU-sovereign-Cloud* часто означає, що регіональна інфраструктура контролюється US-материнською компанією. У сценарії геополітичного напруження або розширення санкцій ця *суверенна* хмара може стати недоступною з юридичних причин, навіть якщо технічно все працює. Розділ 10 розглядає цей ризик глибше.

> *Жоден сертифікат, жоден договір про обробку даних на замовлення (AVV), жоден маркетинговий ярлик про «суверенність» чи «EU-сумісність» не замінять власної комплаєнс-архітектури з чітко визначеними відповідальними людьми.*

Антропологічна точка

Комплаєнс часто сприймають як обмеження — те, що додають до системи зверху, щоб задовольнити регулятора. Така перспектива приховує його справжню функцію. Комплаєнс — це структурний шар, який експонує наявні рішення про відповідальність. Якщо у вас немає документованої матриці відповідальності, це не означає, що відповідальності немає. Це означає, що вона не названа і у момент інциденту опиниться там, де її не очікують. Зазвичай — на найслабшій ланці організаційної ієрархії.

Висновок

Архітектурний підхід до комплаєнсу — це конструювання організаційного шару системи з тією ж серйозністю, з якою конструюють її технічний шар. Імена відповідальних, виписані мандати, страхове покриття, діаграма відповідальності, доступна AI-оператору як щоденний робочий документ — а не як файл у архіві юридичного відділу. Якщо все це є — комплаєнс перестає бути ризиком і стає опорою. Якщо немає — будь-яка технічна архітектура стоїть на хисткому ґрунті.

Три питання для власного контексту

1. **Класифікація.** Які з ваших AI-процесів (робочих навантажень) підпадають під високий ризик за EU AI Act? Чи існує для кожного письмова класифікація з обґрунтуванням — і хто її підписав?

2. **Розподіл по модулях.** Чи є матриця відповідальності, яка для кожного модуля (модель, дані, інфраструктура, інтеграція, експлуатація) називає Provider, Deployer і страхове покриття? Якщо ні: які модулі особливо критичні?

3. **Тест на удавану суверенність.** Які комплаєнс-твердження ваших Cloud- або AI-постачальників базуються на маркетингових етикетках, а не на договірно зафіксованих, перевіряних обов'язках? Що відбувається з вашою відповідальністю, якщо їхня *EU-Cloud* стане недоступною?