PRIVACY & AI LAW

The Regulatory Map Every Product Team Meets

[FOUNDERS] [PRODUCT MANAGERS] [DEVELOPERS] [MARKETERS]

[!] DISCLAIMER: General information, not legal advice — current as of November 2026.

Gemini Notebook



THE BORDERLESS SAAS PROBLEM

Code deploys globally. Laws apply locally.

GDPR ART. 3(2)

IF YOUR APP TARGETS OR MONITORS THE BEHAVIOR OF USERS WHERE THEY SIT (PER EDPB GUIDELINES 3/2018), THE REGULATORY REGIME ATTACHES TO THE USER, NOT YOUR SERVER. PHYSICAL PRESENCE IS IRRELEVANT.

BORDERLESS DEPLOYMENT MEANS INSTANT, OVERLAPPING MULTI-REGIME COMPLIANCE.

Gemini Notebook

The Series Roadmap



[You Are Here] Ep 00: The Regulatory Map

Ep 01: GDPR Fundamentals

Ep 02: ePrivacy & Tracking

Ep 03: The US State Patchwork

Ep 04: The EU AI Act

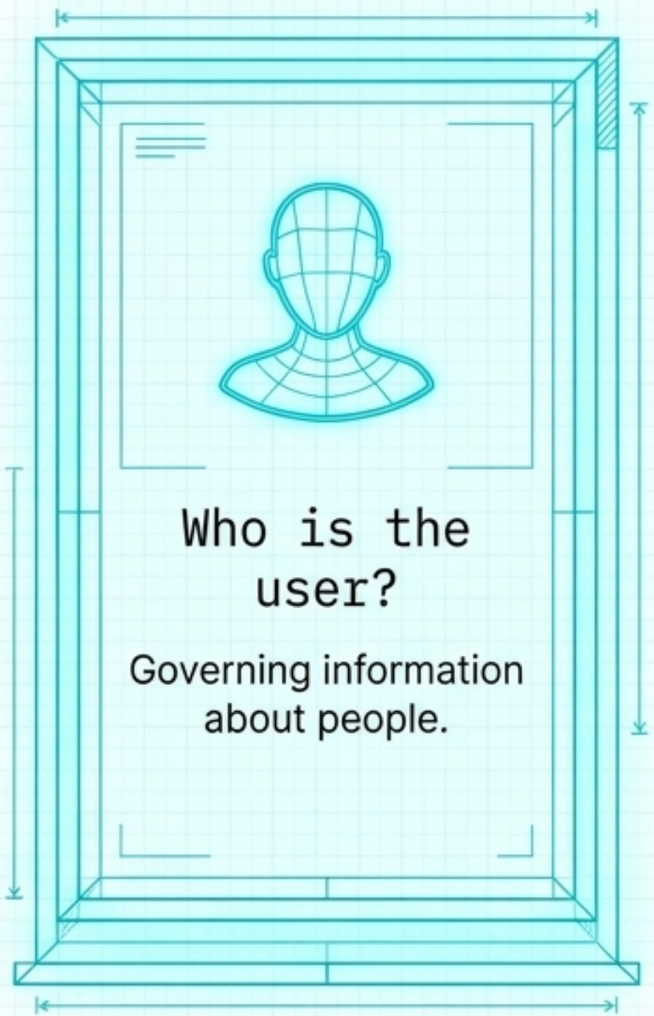
Ep 05: Data Act & DSA

Ep 06: B2B vs. B2C Nuances

Ep 07: Building a Compliance Stack

Gemini Notebook

Stop Conflating the Rules



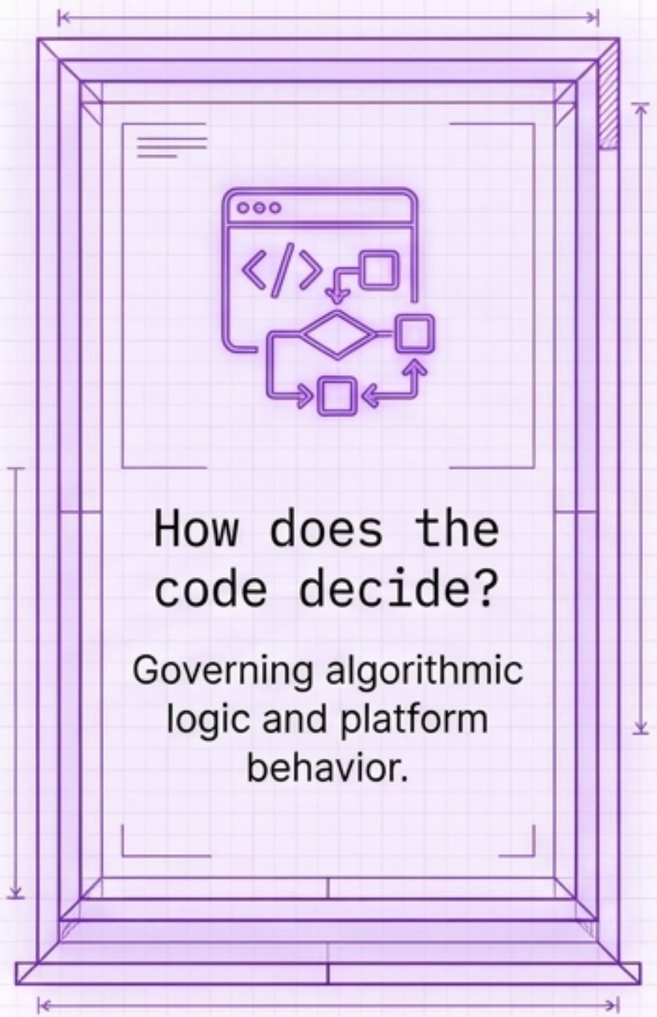
Who is the user?

Governing information about people.



What are you touching?

Governing access to user hardware.

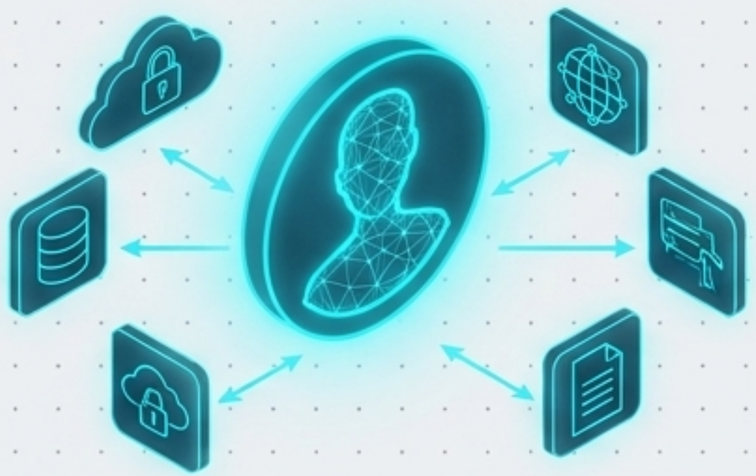


How does the code decide?

Governing algorithmic logic and platform behavior.

Gemini Notebook

(A) Data Protection



Personal Data Protection

Scope: Governs information relating to an identified/identifiable person.

Statutes: EU Charter Arts. 7–8; GDPR 2016/679 Arts. 4–6.

Rule: Requires a lawful basis (e.g., consent, contract) to process.

(B) Device Access



Device Storage & Access

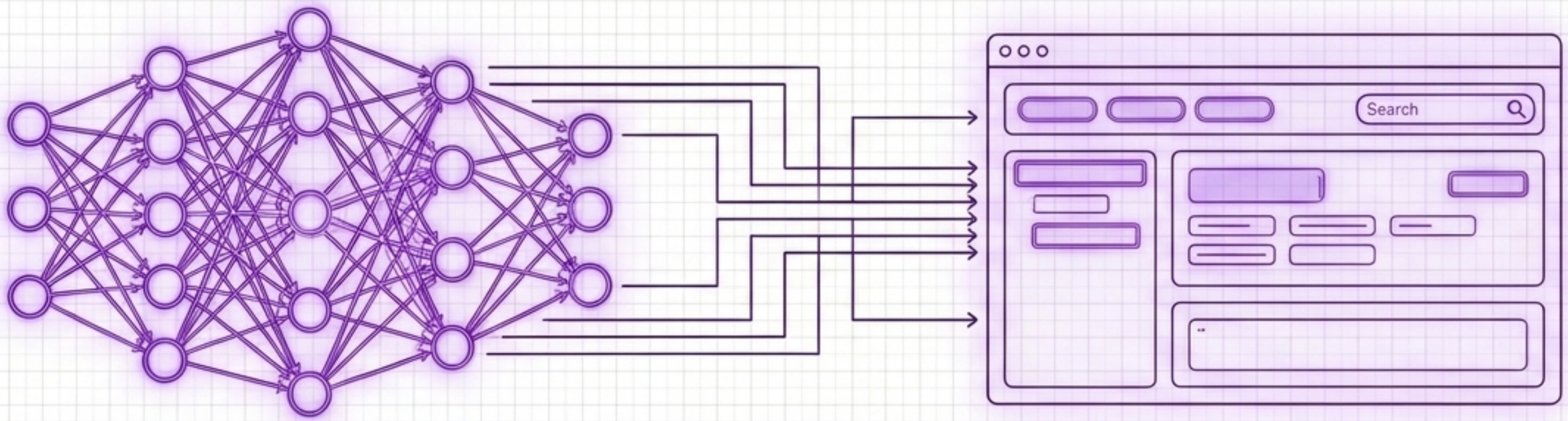
Scope: Governs touching the user's hardware (dropping cookies, reading localStorage), even if the data is totally anonymous.

Statutes: ePrivacy Directive 2002/58/EC Art. 5(3) & 2009/136/EC; EDPB Guidelines 2/2023.

Rule: Requires upfront consent for anything not strictly necessary to provide the requested service.

Gemini Notebook

(C) System Governance & Platform Rules



Core Focus: AI & System Logic

Scope: Governs how algorithms act, evaluate risk, and explain themselves.

Statutes: EU AI Act 2024/1689 & July 2026 Digital Omnibus Regulation 2026/1744.

Adjacent Guardrails

Digital Services Act (DSA): Arts. 25 (bans dark patterns), 26 (ad transparency), 28 (minor protection).

EU Data Act 2023/2854: Ensures users can access and port data generated by connected IoT devices.

Gemini Notebook

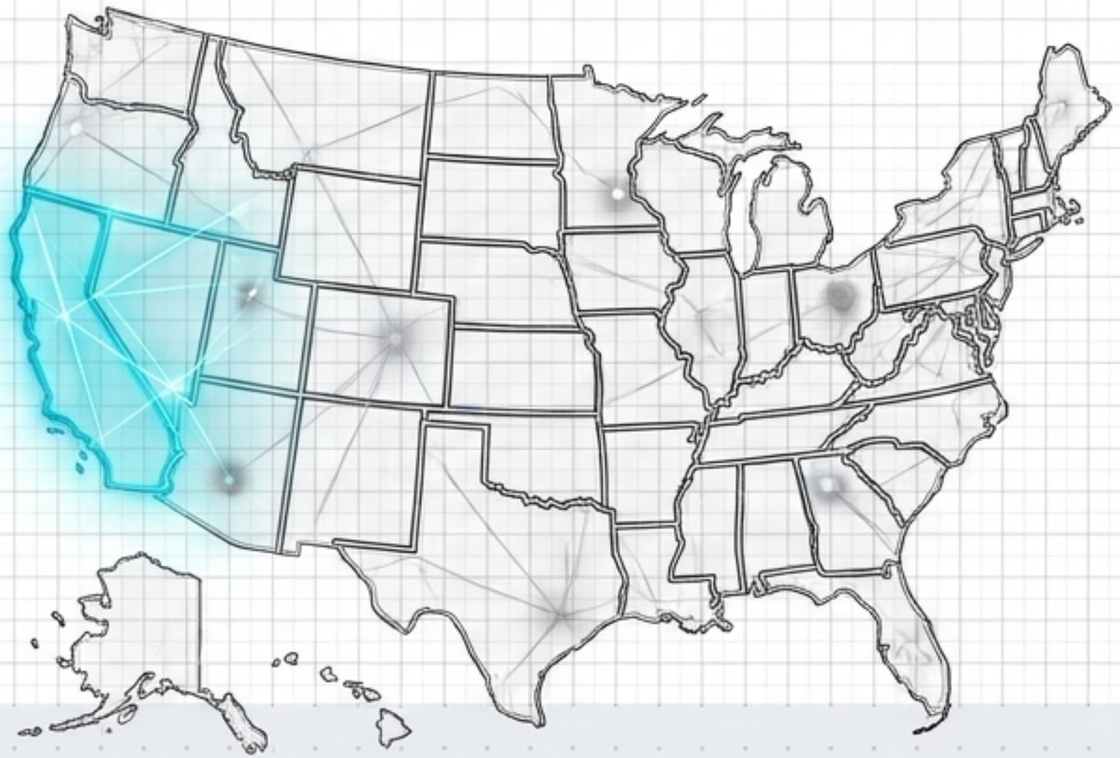
Global Regime Diagnostic: Europe & UK

Regime	Trigger	Default Posture	Regulator
GDPR	Processing personal data	Upfront lawful basis required	National DPAs
ePrivacy	Accessing terminal equipment	Opt-in consent required (unless strictly necessary)	National DPAs / Telecom regulators
AI Act	Placing AI systems on market / putting into service	Risk-tiered conformity (unacceptable, high, transparency, minimal)	National Authorities + European AI Office

Gemini Notebook

Global Regime Diagnostic: United States

US State Patchwork	CCPA/CPRA (Cal. Civ. Code §§ 1798.100–1798.140) + ~20 other states. Posture: Notice-and-Opt-Out (must respect W3C Global Privacy Control (GPC) headers).
US Federal Sectoral Layer	FTC Act Section 5 (deceptive practices), COPPA (children), GLBA (financial), Health Breach Notification Rule.
US AI Posture	Voluntary frameworks (NIST AI RMF, AI RMF Generative AI Profile) focusing on risk mapping, enforced primarily via FTC oversight of deceptive claims.



Gemini Notebook

The Full-Stack Legal Architecture

Compliance isn’t just a legal team signature. It is a distributed engineering requirement.

1. UI/Client Layer — Frontend owns device access

2. API/Logic Layer — Middleware and routing

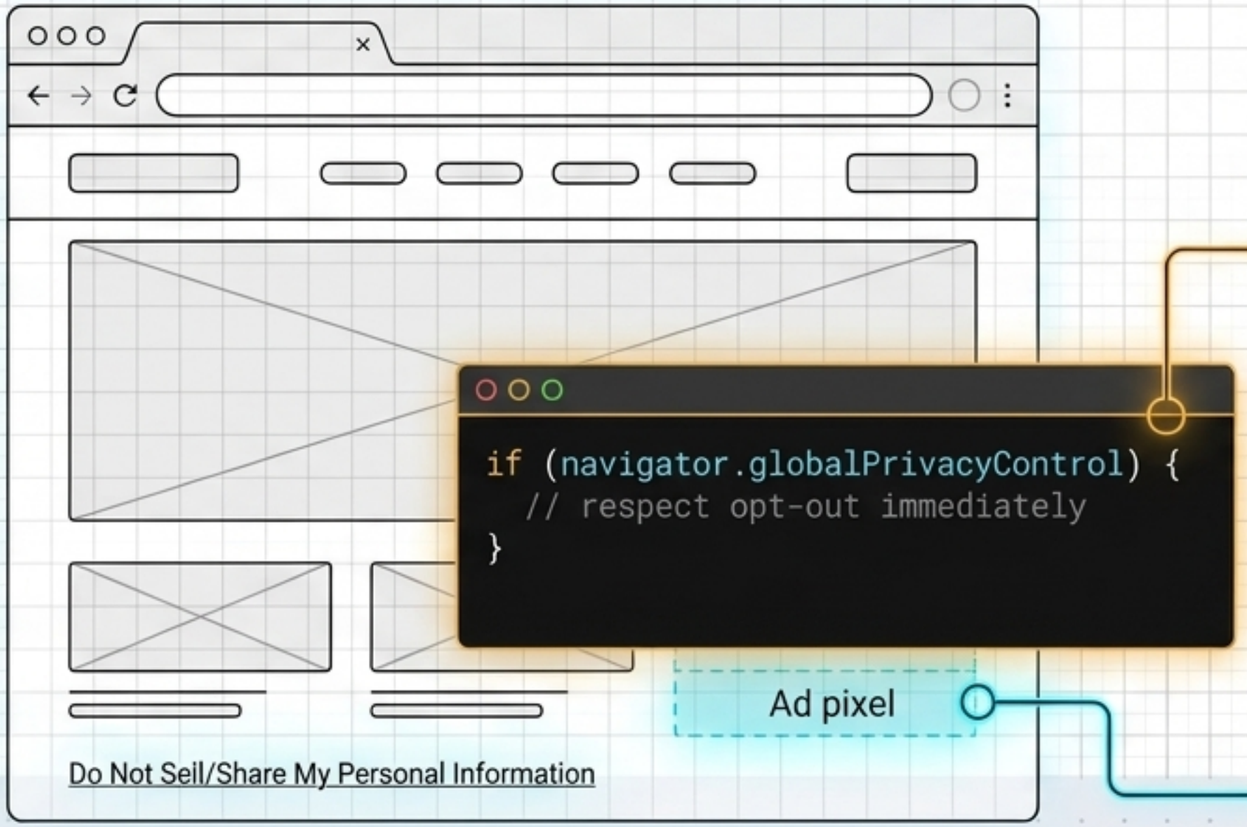
3. Database/Storage Layer — Backend owns data retention

4. AI/ML Models Layer — AI builders own algorithmic transparency



Gemini Notebook

Frontend & Marketing (The UI Layer)



Frontend Engineers:

ePrivacy Art. 5(3): Firing non-essential cookies, localStorage, or third-party SDKs requires prior opt-in.

CCPA: Must listen for and respect Global Privacy Control (GPC) headers automatically.

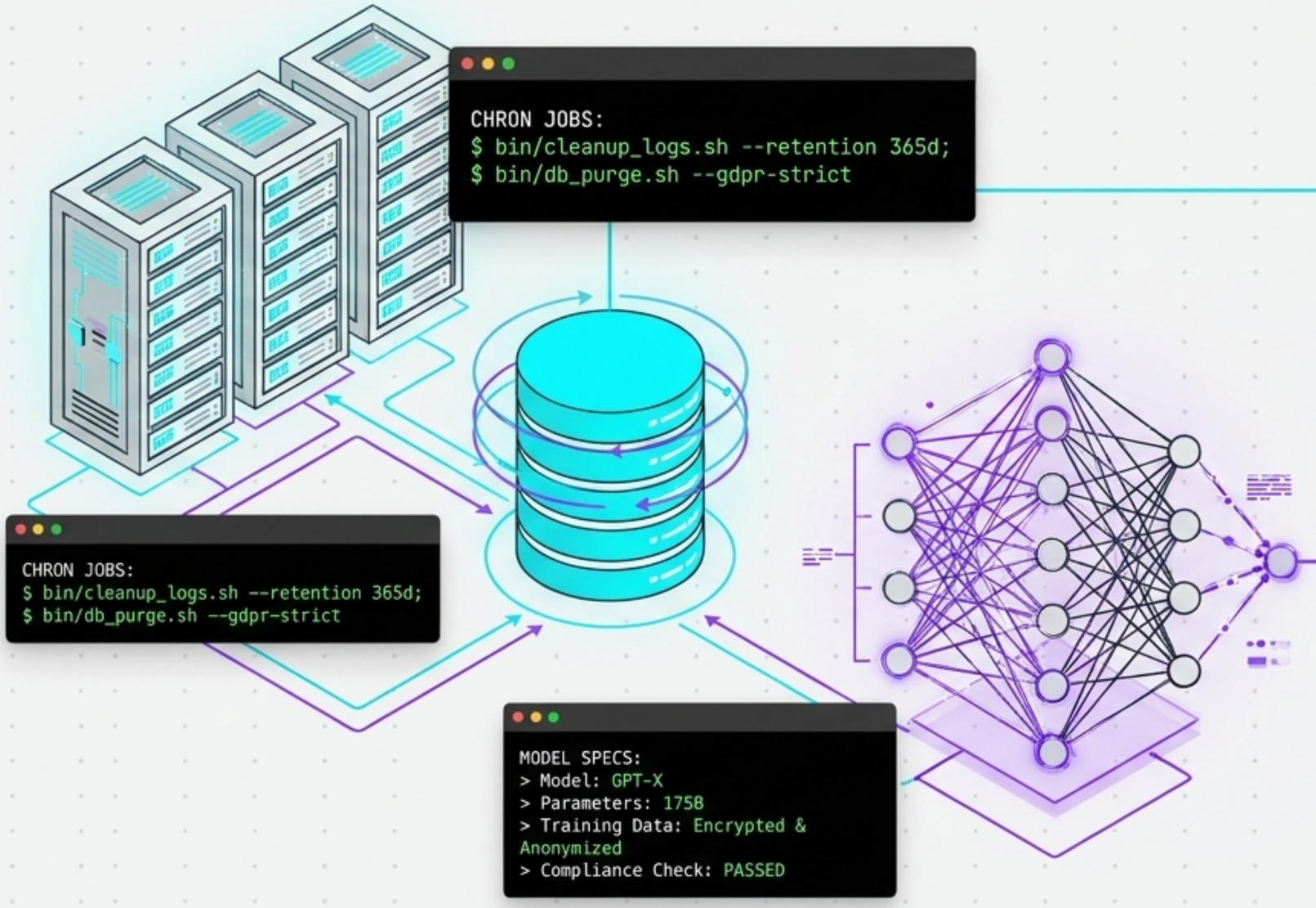
Marketers & Designers:

DSA Art. 25: Zero tolerance for dark patterns in UI consent flows.

CCPA: Must provide clear **Notice at Collection** and **Do Not Sell/Share** links. Ad pixels require compliance mechanisms.

Gemini Notebook

Backend & AI (The Data & Logic Layer)



Backend Engineers:

- **GDPR Art. 5(1)(e):** Databases and logs must enforce strict retention schedules (Storage Limitation).
- **CNIL Developer's Guide:** Mandates secure handling of third-party APIs and encrypted data transit.

AI Builders:

- **GDPR:** Training data vs. prompt injections—user inputs are personal data.
- **AI Act:** Model transparency labeling and strict avoidance of prohibited practices (e.g., untargeted scraping for facial recognition).

Gemini Notebook

End-to-End Worked Product Scenario

The Product: A cross-border B2B/B2C productivity app with an embedded AI assistant.



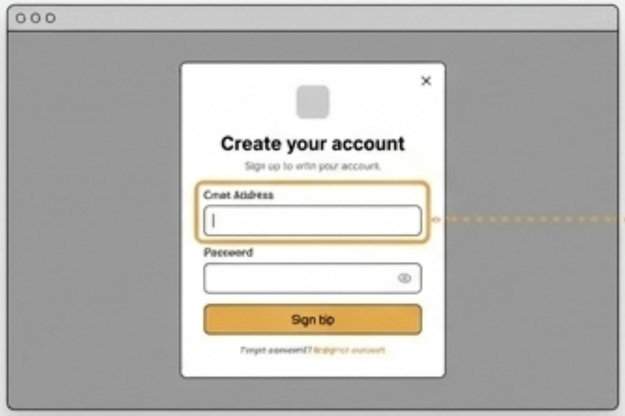
Stage 1: Landing Page Visit → Stage 2: Account Creation → Stage 3: AI Chat Interaction

Tracing a **single user journey** from **first visit to AI interaction**, mapping the legal triggers at every node.

Gemini Notebook

Stage 1 & 2: Landing Page to Account Creation





Stage 1: The Landing Visit

Trigger: The first tracker drop.

Law: ePrivacy Art. 5(3) demands opt-in for EU users. Meanwhile, a California user's browser sends a GPC signal which must be honored immediately to prevent data sale/sharing.

Stage 2: Account Creation

Trigger: User types their email.

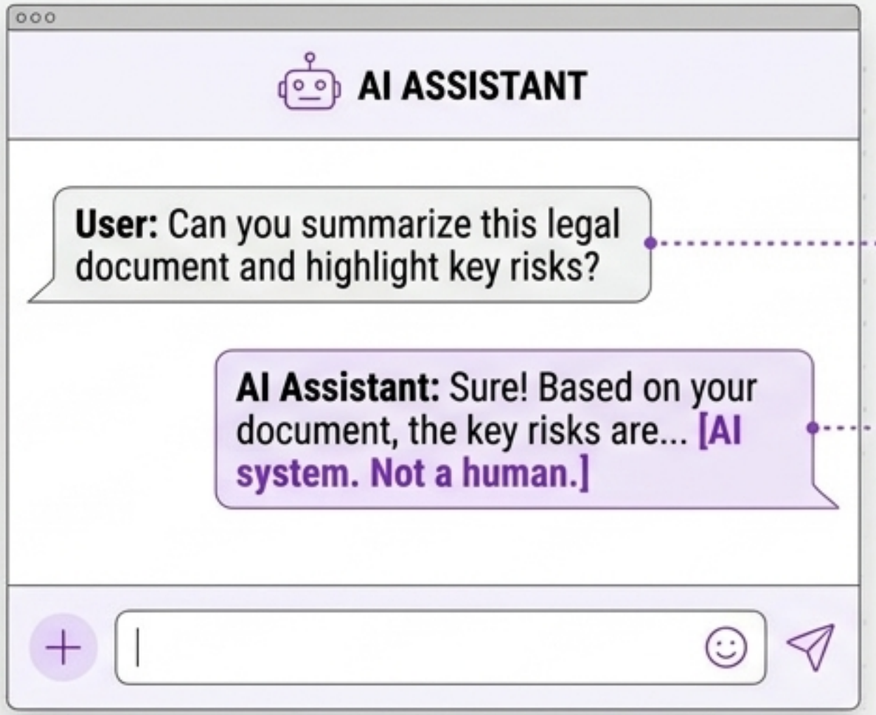
Law: GDPR Art. 6 requires a lawful basis (Contract) to process the account data. CCPA requires a Notice at Collection at or before the point of data entry.

Stage 1: Landing Page Visit → Stage 2: Account Creation → Stage 3: AI Chat Interaction

Tracing a **single user journey** from **first visit to AI interaction**, mapping the legal triggers at every node.

Gemini Notebook

Stage to Stage 3: AI Chat Interaction



EU AI Act Art. 50 (live Aug 2026):

Mandatory transparency. The UI must explicitly inform the user they are interacting with an AI system, not a human.

GDPR Intersection:

Personal data entered into the prompt (or generated as output) remains subject to GDPR. Per EDPB Opinion 28/2024 & Statement 3/2024, AI providers must have a lawful basis for processing inputs and cannot use personal data prompts for model retraining without explicit consent.

Stage 1: Landing Page Visit → Stage 2: Account Creation → Stage 3: AI Chat Interaction

Tracing a **single user journey** from **first visit to AI interaction**, mapping the legal triggers at every node.

Gemini Notebook

Common Startup Myths Debunked

Myth: B2B data isn't covered.

Reality: False. Business emails (john@company.com) are personal data under GDPR.

Myth: US incorporation shields us.

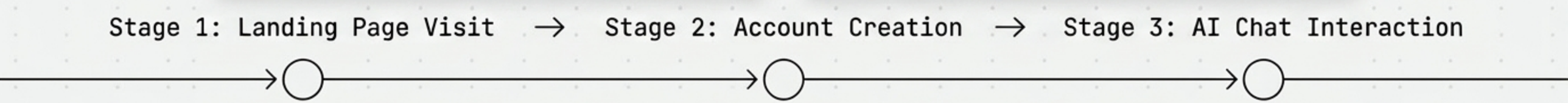
Reality: False. GDPR Art. 3(2) extraterritoriality applies if you monitor EU users.

Myth: The US has no privacy law.

Reality: False. You face a strict state patchwork (CCPA/CPRA) + FTC federal enforcement.

Myth: The AI Act replaces GDPR.

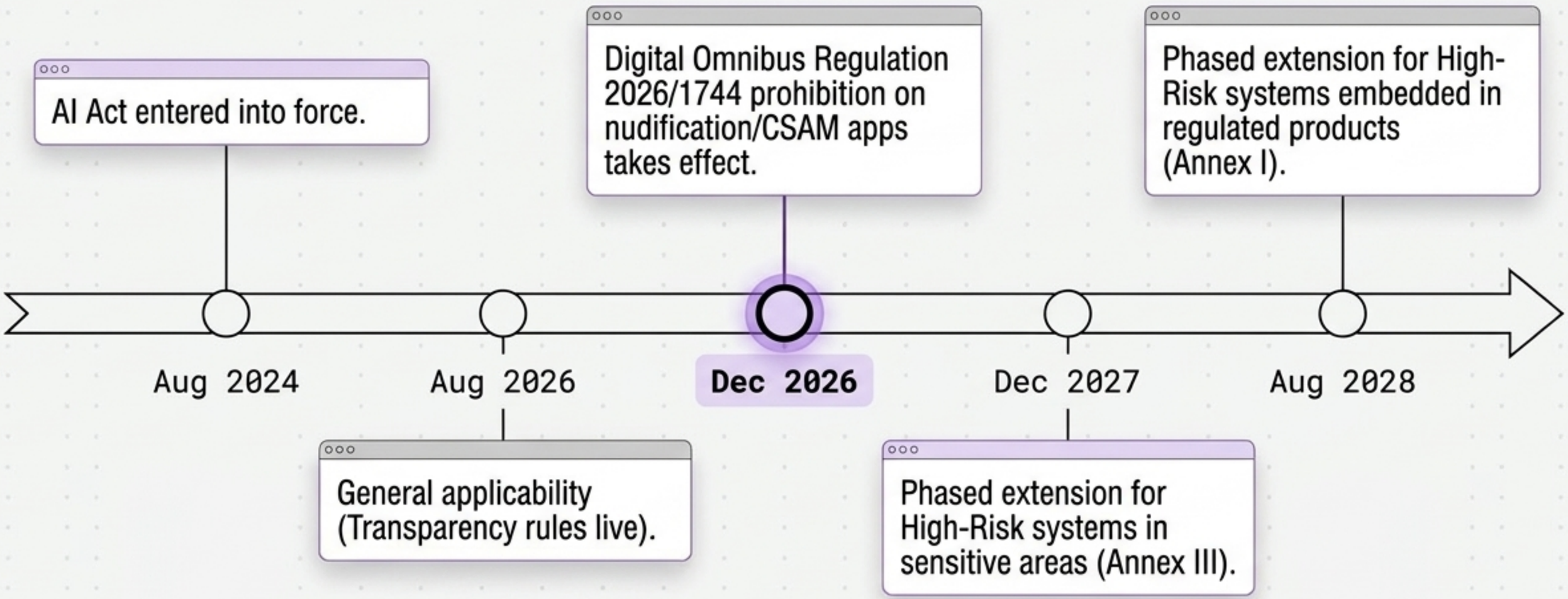
Reality: False. They apply cumulatively. Data laws govern the input; AI laws govern the logic.



Tracing a **single user journey** from **first visit to AI interaction**, mapping the legal triggers at every node.

Gemini Notebook

The Moving Targets: AI Act Timelines (2026–2028)

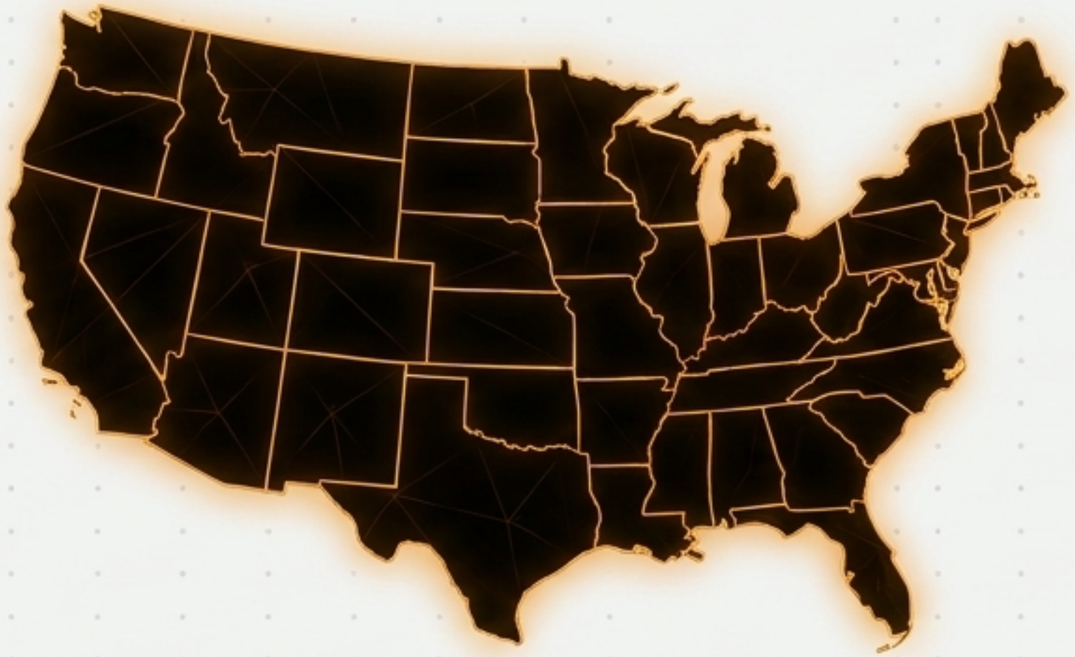


Tracing a **single user journey** from **first visit to AI interaction**, mapping the legal triggers at every node.

Gemini Notebook

Regulator Nuances & Fragmentation





National ePrivacy Variations.

While the EU has unified GDPR, ePrivacy enforcement varies by country. (e.g., France's CNIL is historically stricter on analytics cookies compared to the UK ICO's pragmatic guidance).

The US State Shifting Sands.

CCPA is just the beginning. Nearly half of US states now have comprehensive privacy statutes, with varying thresholds for data brokers and algorithmic opt-outs.

Gemini Notebook

Four Foundational Questions Before Shipping

PRE-FLIGHT CHECKLIST :: COMPLIANCE_ENGINE v3.0

1. **Where is the user?**
   Determines jurisdiction: EU vs. US State vs. Global.

2. **Are we identifying them?**
   Triggers GDPR/CCPA personal data rules.

3. **Are we touching their device?**
   Triggers ePrivacy/cookie/tracker rules.

4. **Is an algorithm deciding or generating?**
   Triggers AI Act transparency and risk tiering.

Gemini Notebook

The Red Lines: When to Call Legal

Stop building and consult qualified counsel if a feature involves:

- Processing special categories of data (health, biometric, union membership per GDPR Art. 9).
- Deploying AI for biometric categorization, emotion recognition, or social scoring (Prohibited under AI Act Art. 5).
- Selling or sharing data without a robust, automated opt-out mechanism (CCPA).
- Scraping the internet to expand facial recognition databases.

Gemini Notebook

Up Next

Episode 01: GDPR Fundamentals

Deep dive into lawful bases, data mapping, and the right to be forgotten.

```
[ !] DISCLAIMER: General information, not legal advice — current as of November 2026.
```

Gemini Notebook