PRIVACY & AI LAW — S06E03: COOKIES, TRACKERS & CONSENT BANNERS DONE PROPERLY

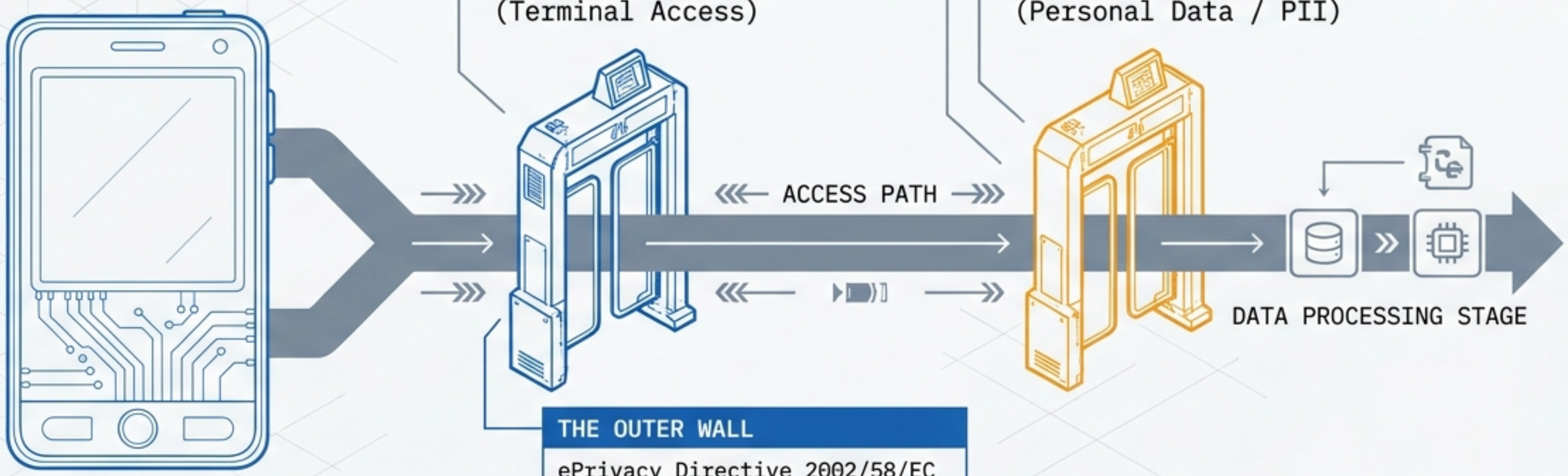
The Builder’s Blueprint for UX, Engineering, and Marketing.



General information, not legal advice — current as of November 2026.

Gemini Notebook

EPISODE 2 RECAP: GDPR governs Personal Data/PII.
But tracking starts before data becomes personal.

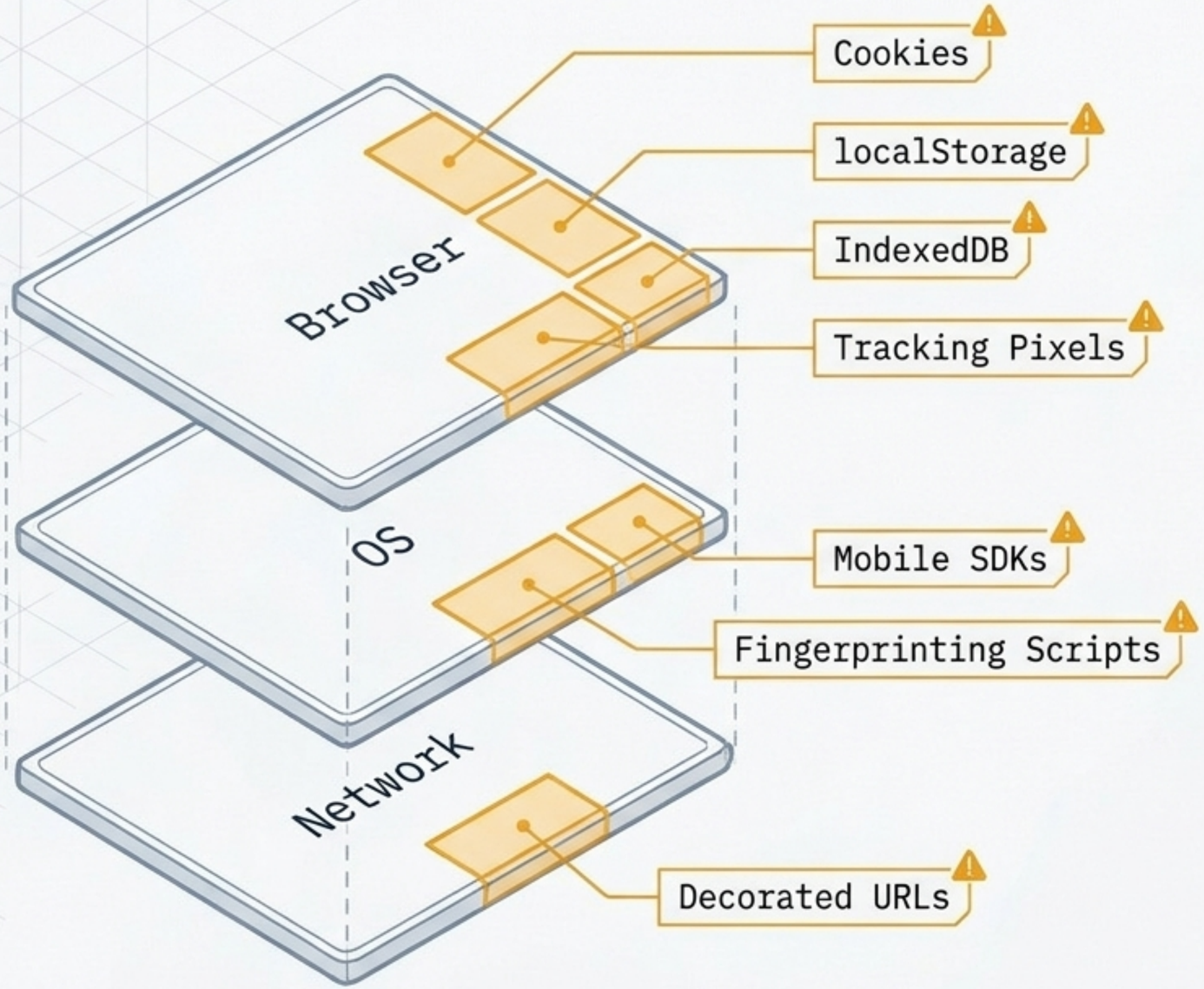


THE OUTER WALL

ePrivacy Directive 2002/58/EC Art. 5(3) & 2009/136/EC (and UK PECR Reg. 6) guard the physical device.

THE MANDATE: Storing or accessing any information on a user's terminal equipment requires prior, informed consent unless strictly necessary.

Gemini Notebook



CJEU Planet49 (C-673/17)

Confirms Art. 5(3) applies regardless of whether the data accessed is personal.

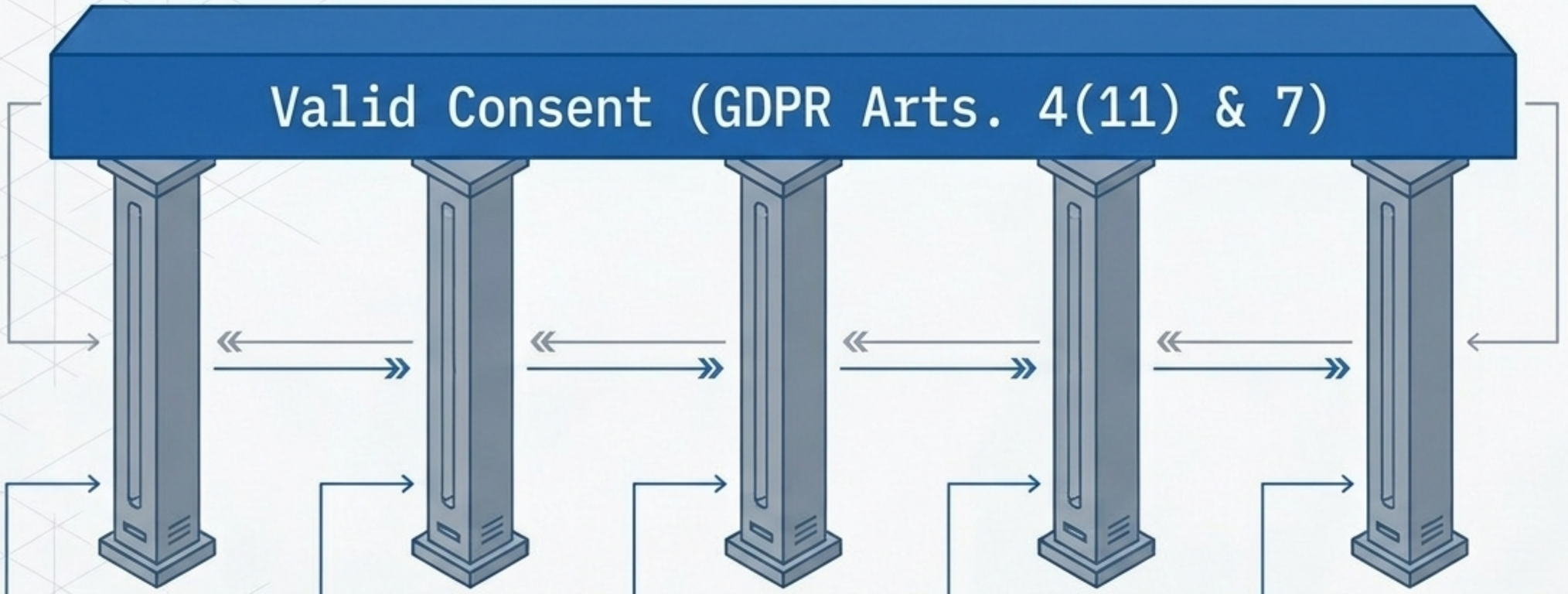
EDPB Guidelines 2/2023 & CNIL Mobile Recommendations

The law explicitly covers all modern frontend and mobile tracking mechanisms.

If it reads or writes to or writes to the device, it is caught.

Gemini Notebook

Valid Consent (GDPR Arts. 4(11) & 7)



Freely Given:

No deceptive cookie-walls (EDPB 05/2020).

Access cannot be **strictly conditional** on non-necessary tracking.

Specific & Informed:

Granular purpose choices; clear identity of controllers.

Unambiguous Prior Action:

Active physical opt-in. No pre-ticked boxes (CJEU Planet49); no scroll-to-consent.

Easy Withdrawal:

Must be as easy to withdraw as it was to give (Art. 7(3)).

Demonstrable:

Backend logging of consent proof (Art. 7(1)).

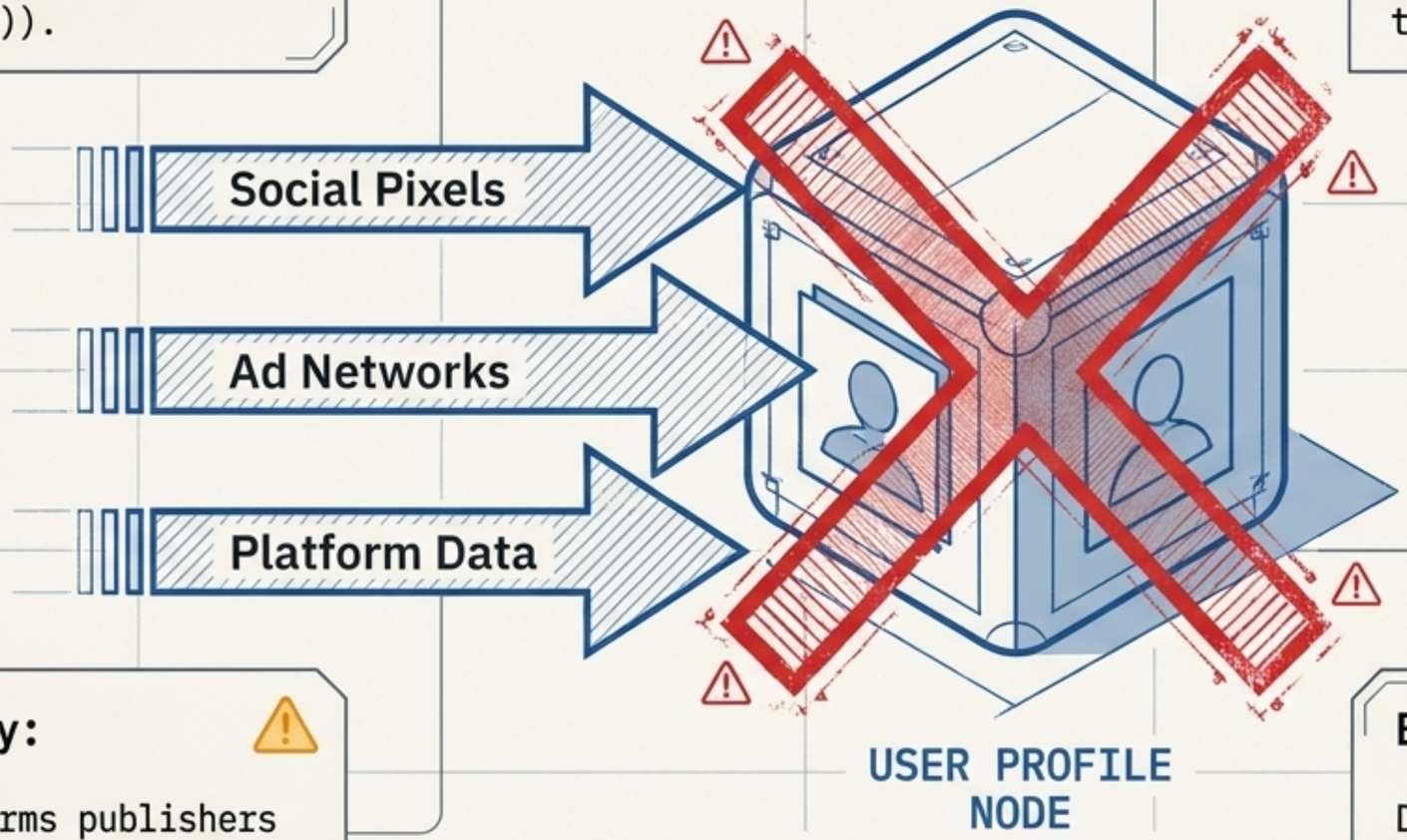
Gemini Notebook

The Rule:

Behavioural tracking and targeted ads cannot rely on contract necessity or legitimate interest (GDPR Art. 6(1)(f)).

The Precedents:

CJEU Meta v Bundeskartellamt (C-252/21) & EDPB Guidelines 1/2024 definitively close this loophole.



Joint Liability:

EDPB 8/2020 confirms publishers and ad-tech (e.g., social pixels) are joint controllers for the collection phase.

Big Tech Lock-In:

DMA Art. 5(2) legally prohibits gatekeepers from combining core platform data without explicit GDPR consent.

Gemini Notebook

Exempt / Strictly Necessary	Prior Consent Required
Session/Auth: Exempt (Load balancing, login tokens)	**Third-Party Analytics:** Opt-In Mandatory (Cross-site measurement)
Cart/Checkout: Exempt (Remembering basket items)	**Ad/Remarketing Pixels:** Opt-In Mandatory (Meta Pixel, Google Ads)
Security: Exempt (Strictly scoped fraud detection)	
UI Preferences: Exempt (Language selection, accessibility settings)	

Gemini Notebook

First-Party Analytics



CNIL Sheet n°16

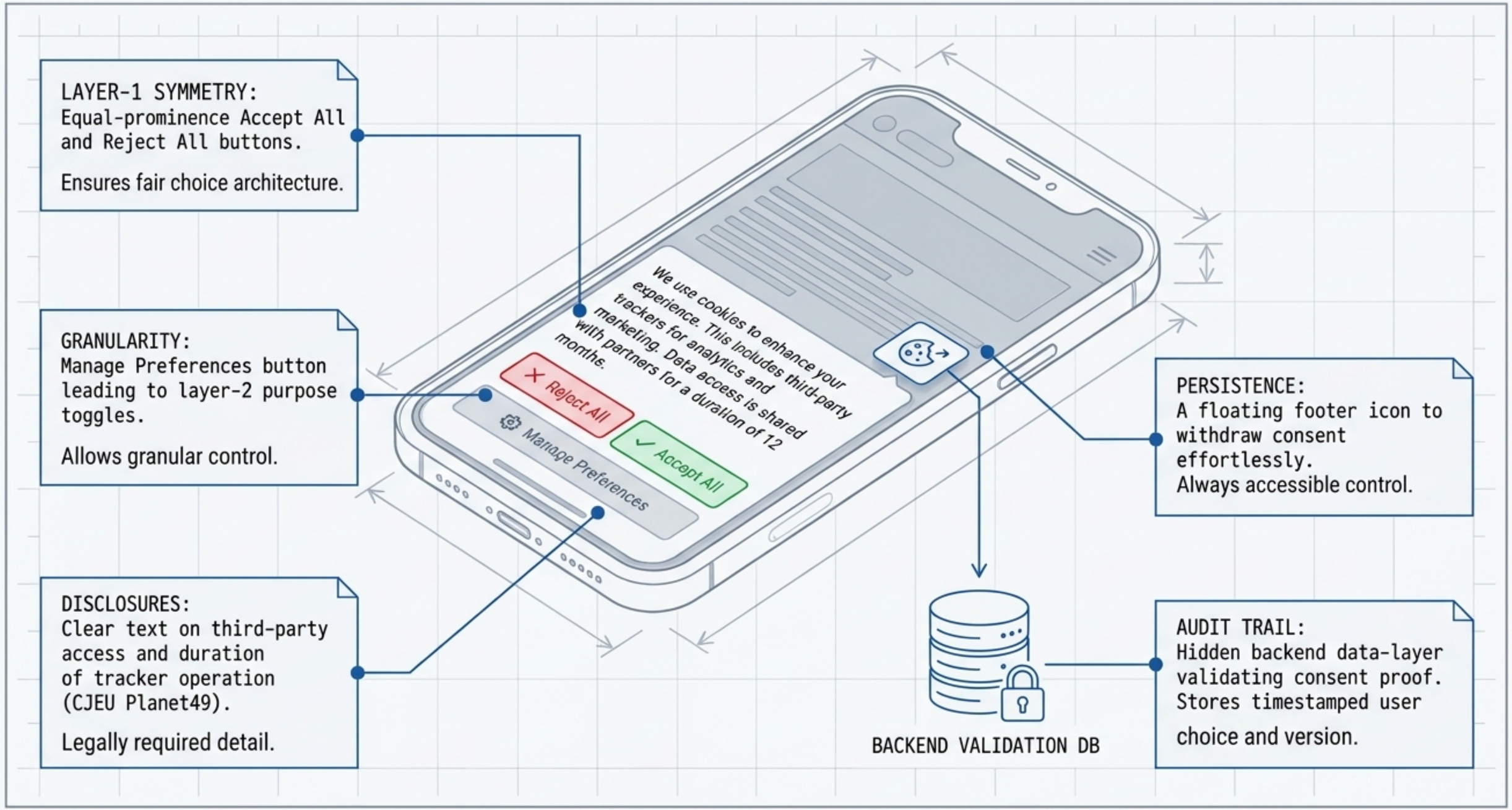
Exempt ONLY IF: Strictly limited to anonymous aggregate performance, first-party only, no cross-site tracking, and no data sharing with the vendor.



Stricter Regimes (e.g., UK ICO)

Opt-In Mandatory: Treat as optional. Analytics, even first-party, require prior consent unless the upcoming ePrivacy Regulation changes the baseline.

Gemini Notebook

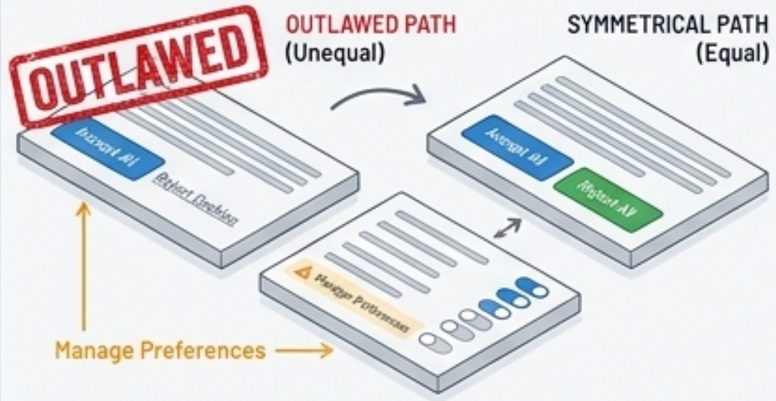


Gemini Notebook

BANNED UI DESIGNS (DARK PATTERNS)

Overloading & Obstructing

(EDPB Cookie Banner Taskforce, CPPA Advisory 2024-02)



Hiding 'Reject' in text links or moving it to layer 2.

Deceptive Contrast

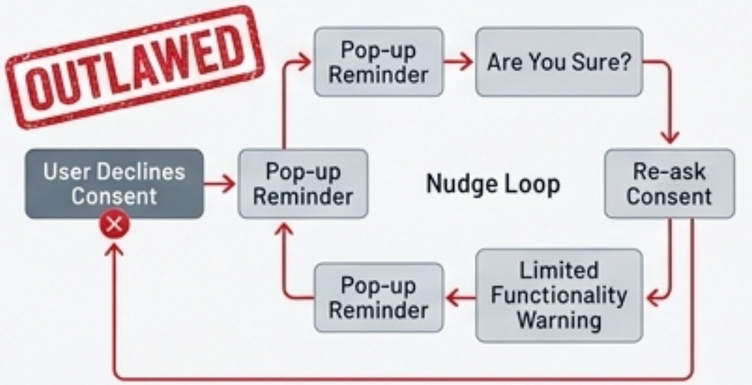
(FTC Dark Patterns Report)



Greyed-out or invisible reject buttons.

Fickle / Stirring

(EDPB Guidelines 03/2022)

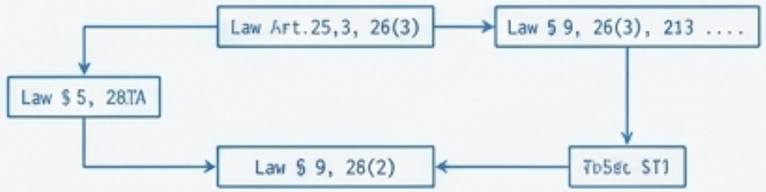


Nudging or repeatedly asking after a user declines.

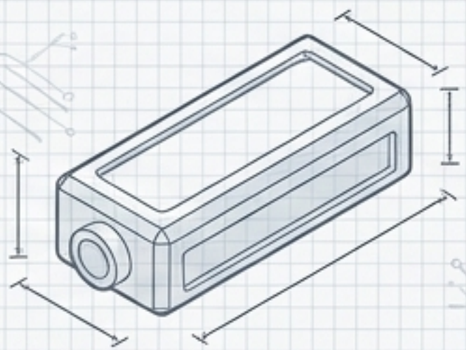
Regulatory Backing



DSA Arts. 25, 26(3) & 28(2) strictly prohibit manipulating users via interface design.

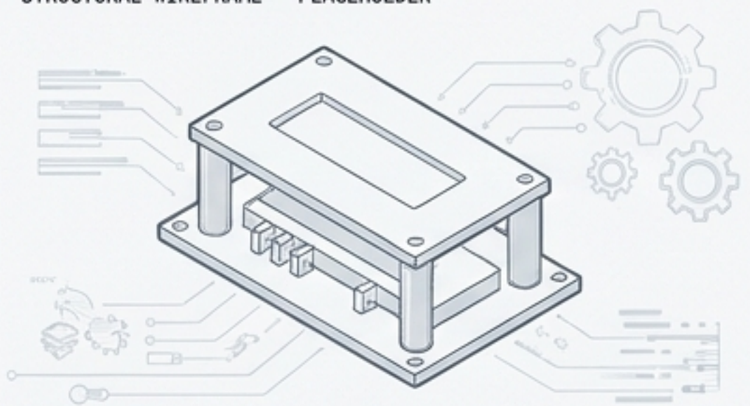


STRUCTURAL WIREFRAME - PLACEHOLDER



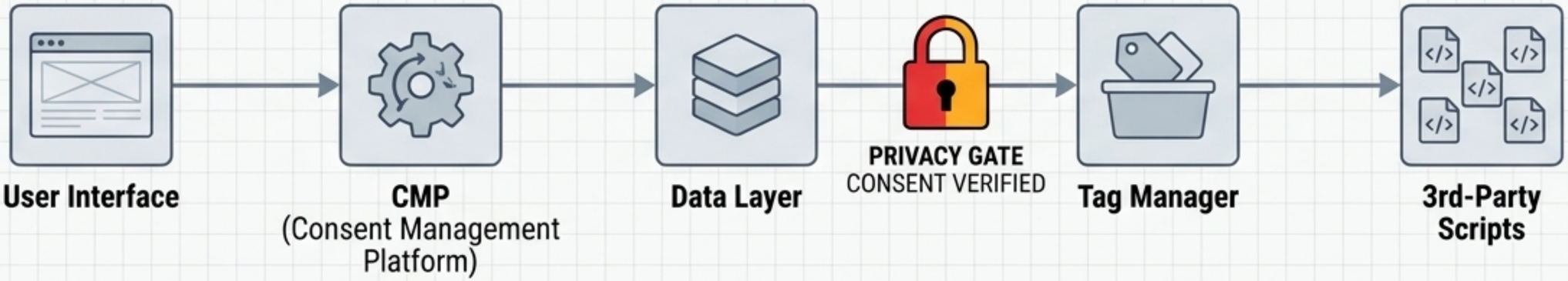
FUTURE REGULATION MAPPING

STRUCTURAL WIREFRAME - PLACEHOLDER



COMPLIANCE PATHWAY DESIGN

Gemini Notebook



Engineering Directives (CNIL Developer Guide & Art. 25 EDPB 4/2019)

Block by Default

Scripts, SDKs, and pixels must be technically blocked from firing before verified opt-in.
(Technical Failure: Critical Red)

- Code Snippet:

```
const consentState = fetchConsent();
if (!consentState.isOptIn) {
  return;
}
```

State Verification

Gate server-side forwarding based entirely on the verified consent state payload.
(Structural Wireframe: Blueprint Blue)

- Code Snippet:

```
function sendServerPayload(data) {
  const verifiedState = validatePayloadState(data);
  if (verifiedState) {
    processForwarding(data);
  } else {
    return null;
  }
}
```

Privacy by Design

Hardcode consent logic into the codebase architecture—do not rely solely on third-party asynchronous wrappers.
(Structural Wireframe: Blueprint Blue)

- Code Snippet:

```
class PrivacyModule {
  constructor() {
    this.consentManager = new HardcodedConsentManager();
  }
  execute(feature) {
    if (this.consentManager.isAuthorized(feature)) {
      feature.run();
    }
  }
}
```

Gemini Notebook

GLOBAL PRIVACY CONTROL (GPC): AUTOMATED OPT-OUT SIGNAL

HTTP Request Header

```
1  GET /resource HTTP/1.1
2  Host: example.com
3  User-Agent: Mozilla/5.0
4  Accept-Language: en-US,en;q=0.5
5  Sec-GPC: 1
6  Accept: */*
```

AUTOMATED REJECT ALL STATE MACHINE



Signal Detected → CMP Logic Activated

↓

Suppress Tracking Scripts (No Banner Interaction)

Automatically Suppress Tracking Scripts

THE STANDARD

GPC is a W3C specification allowing users to signal opt-out universally at the browser level.

THE IMPLEMENTATION

US frameworks (e.g., CCPA/CPRA) increasingly mandate automated opt-out recognition.

THE ENGINEERING RULE

If Sec-GPC: 1 is detected in the header, CMPs must automatically suppress tracking scripts without requiring the user to manually click 'Reject' on a banner.

Gemini Notebook

THE MODEL

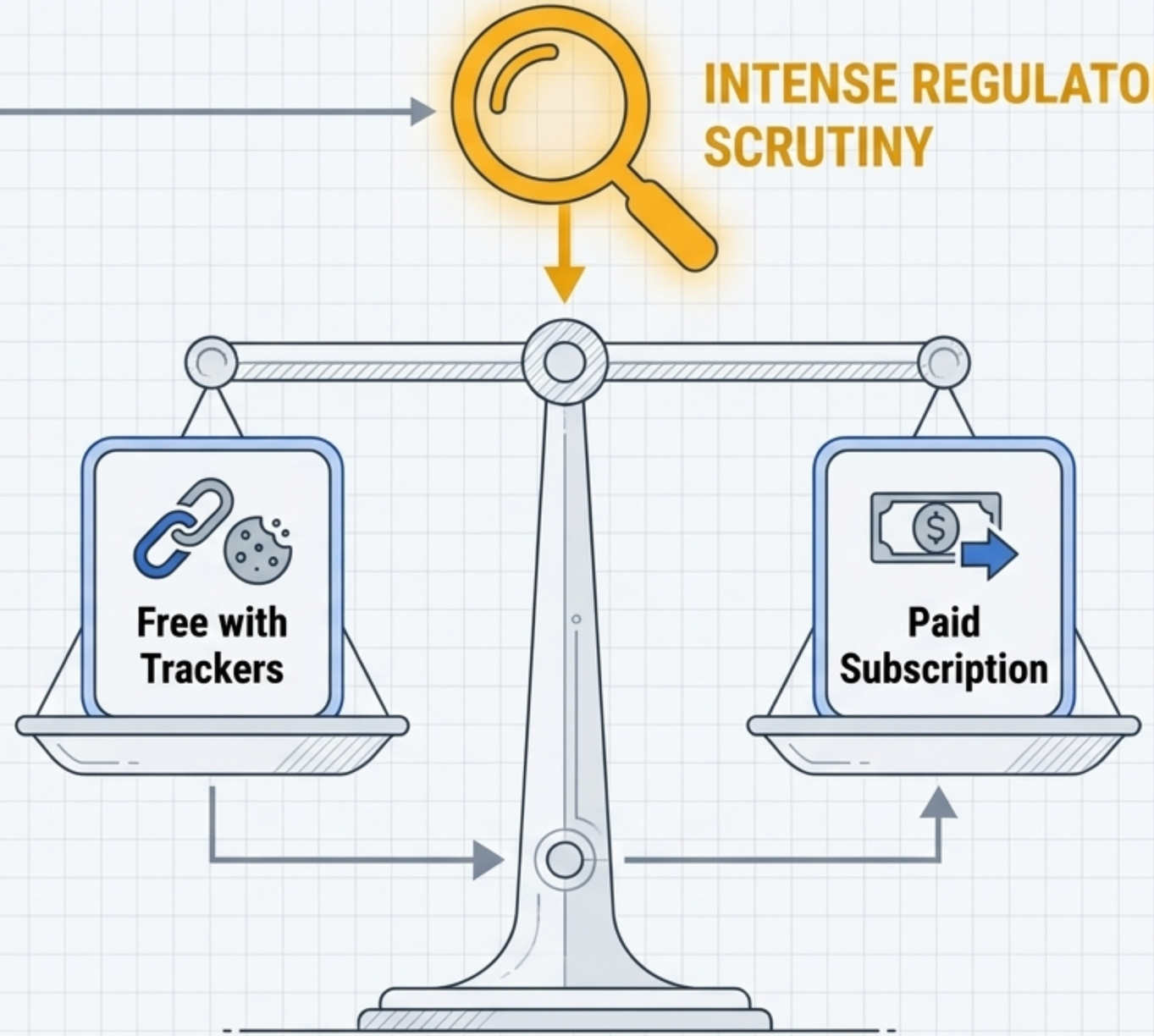
Offering users a binary choice: accept behavioral tracking or pay a subscription fee.

THE REGULATORY MINEFIELD

EDPB Opinion 08/2024 states large or dominant platforms face heavy scrutiny.

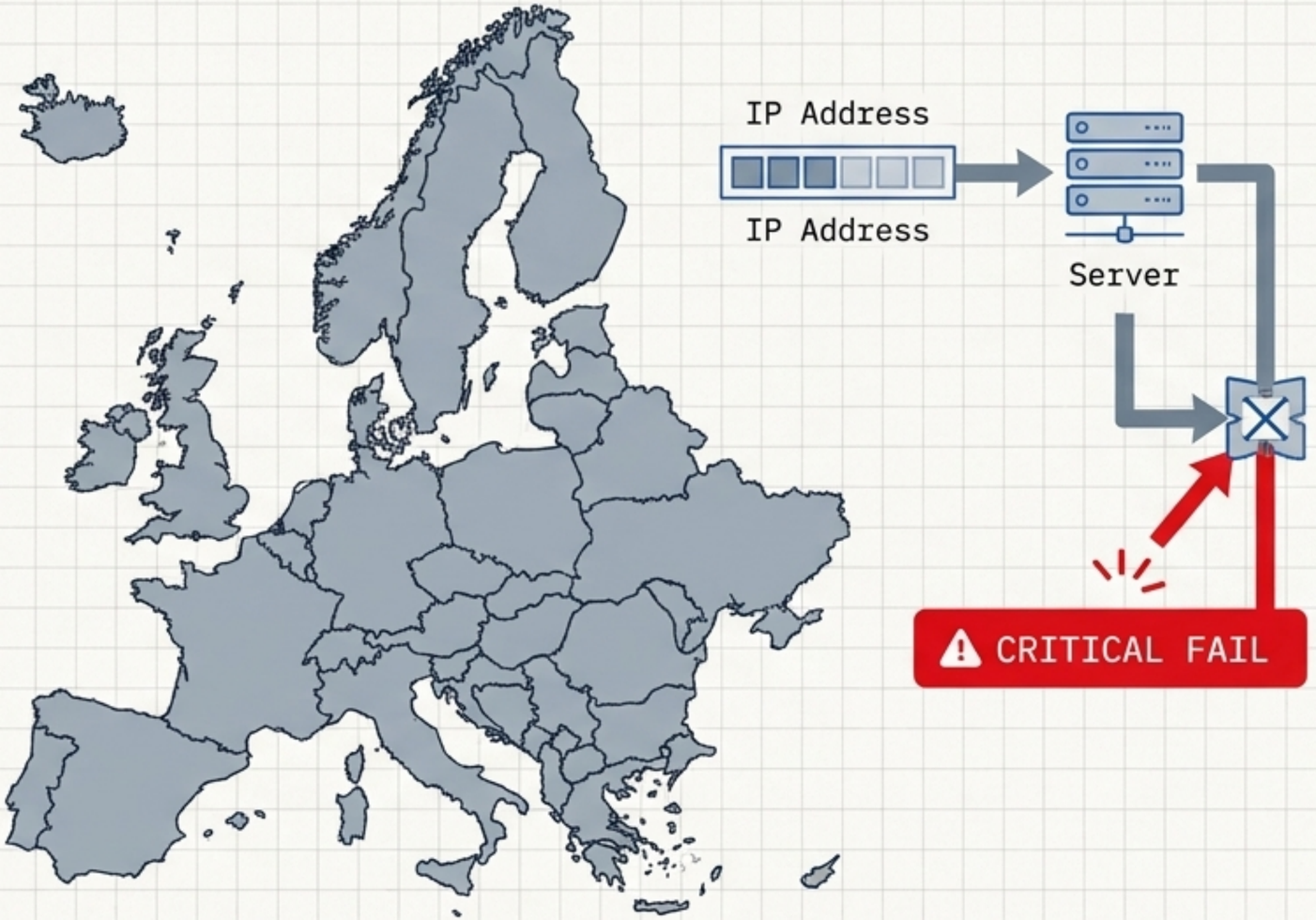
THE VERDICT

Binary tracking-vs-fee walls are unlikely to meet the 'freely given' standard of GDPR without offering a fair, non-tracking, non-paid alternative.



Gemini Notebook

SERVER-SIDE TRACKING & REGIONAL FRAGMENTATION RISKS



SERVER-SIDE & IP EVASIONS

Moving tracking server-side or using IP/fingerprinting workarounds does not bypass the law. EDPB Guidelines 2/2023 explicitly catch these access methods.

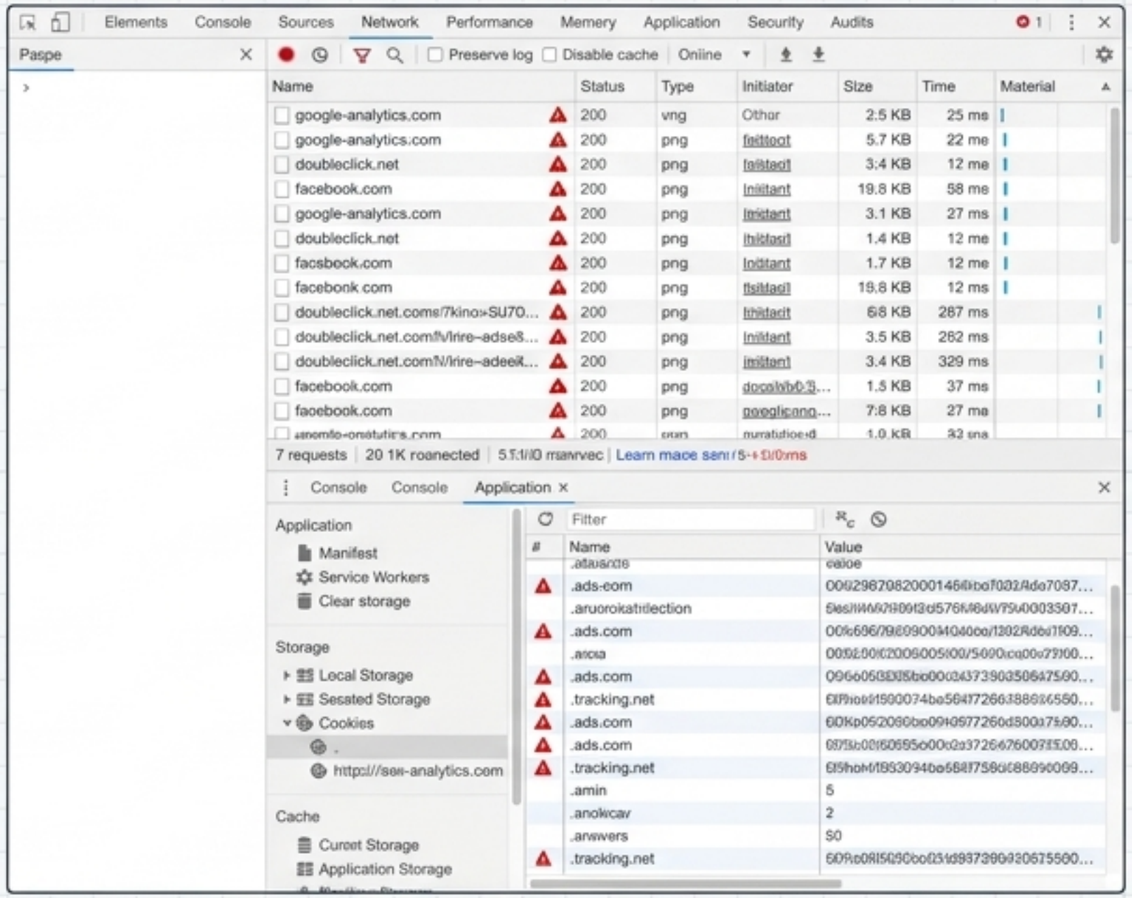
NATIONAL DIVERGENCES

UK vs. EU fragmentation.

The UK ICO enforces a strict opt-in for all analytics, whereas CNIL (France) permits narrow, strictly scoped first-party exemptions.

Know your deployment region.

Gemini Notebook



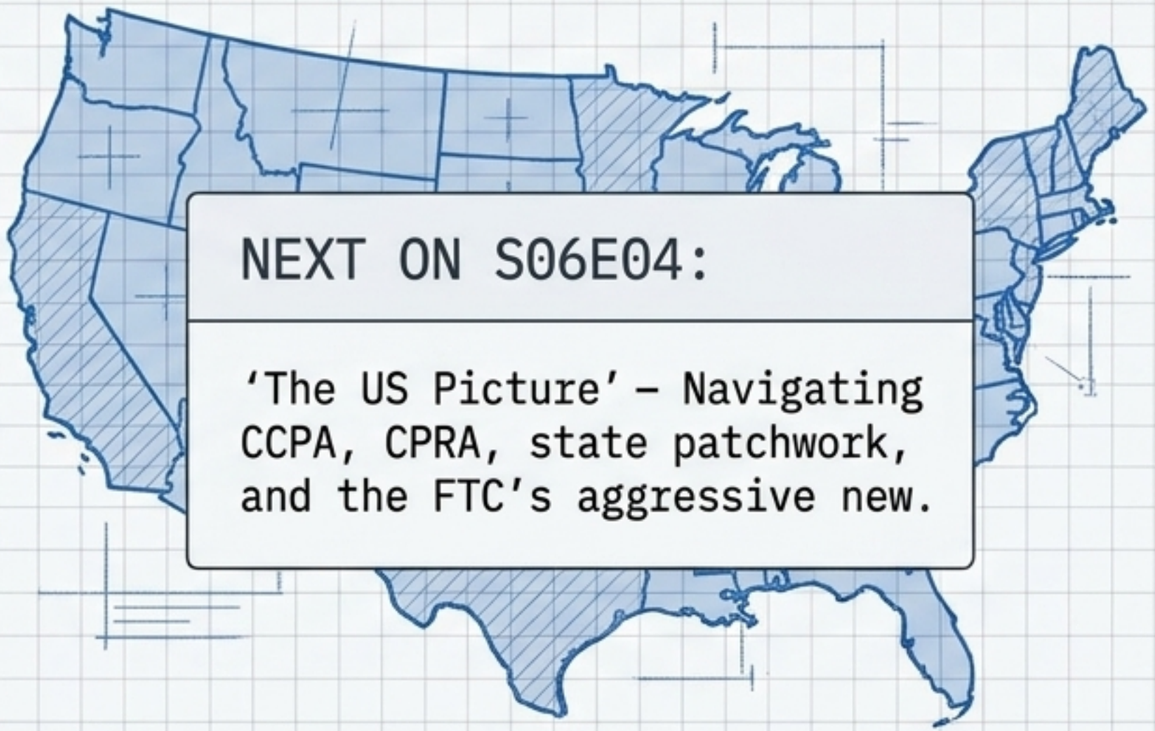
THE 10-MINUTE DEVTOOLS AUDIT

- [ ] **Clear site data**, load page. Do any analytics/ad network requests fire? (Fail if yes). — CRITICAL FAIL
- [ ] Check **Application > Local Storage / Cookies**. Are only strictly necessary items present before click? (Fail if no). — CRITICAL FAIL
- [ ] Click **'Reject All'**. Does anything new load in the Network tab? (Fail if yes). — CRITICAL FAIL
- [ ] Is the 'Reject All' button the exact same size/contrast as 'Accept All'? (Fail if no). — CRITICAL

Gemini Notebook

CONSULT LEGAL COUNSEL IMMEDIATELY IF:

- Implementing Consent-or-Pay walls.
- Integrating joint-controller social pixels (Meta/TikTok).
- Monetising via complex ad-tech bidding.
- Operating platforms directed at children.



NEXT ON S06E04:

'The US Picture' – Navigating CCPA, CPRA, state patchwork, and the FTC's aggressive new.

General information, not legal advice – current as of November 2026.

Gemini Notebook