~/Privacy-AI-Law/S06E07.sh

A Practical Launch Checklist for Small Product Teams

// Built for Founders, PMs, Devs & Marketers

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

Gemini Notebook



Gemini Notebook

Statutes are for courts. **Habits** are for teams.



REGULATOR SOURCE FILTER

EDPB SME Guide | UK ICO SME Web Hub | CNIL Developer Guide | NIST Privacy Framework

Transform compliance from a blocker into a standard QA workflow.

To Do	In Progress	
Privacy Review	Consent Flow QA	Data Mapping Update
Deletion Script Test	Access Control Check	DPIA Trigger

Gemini Notebook

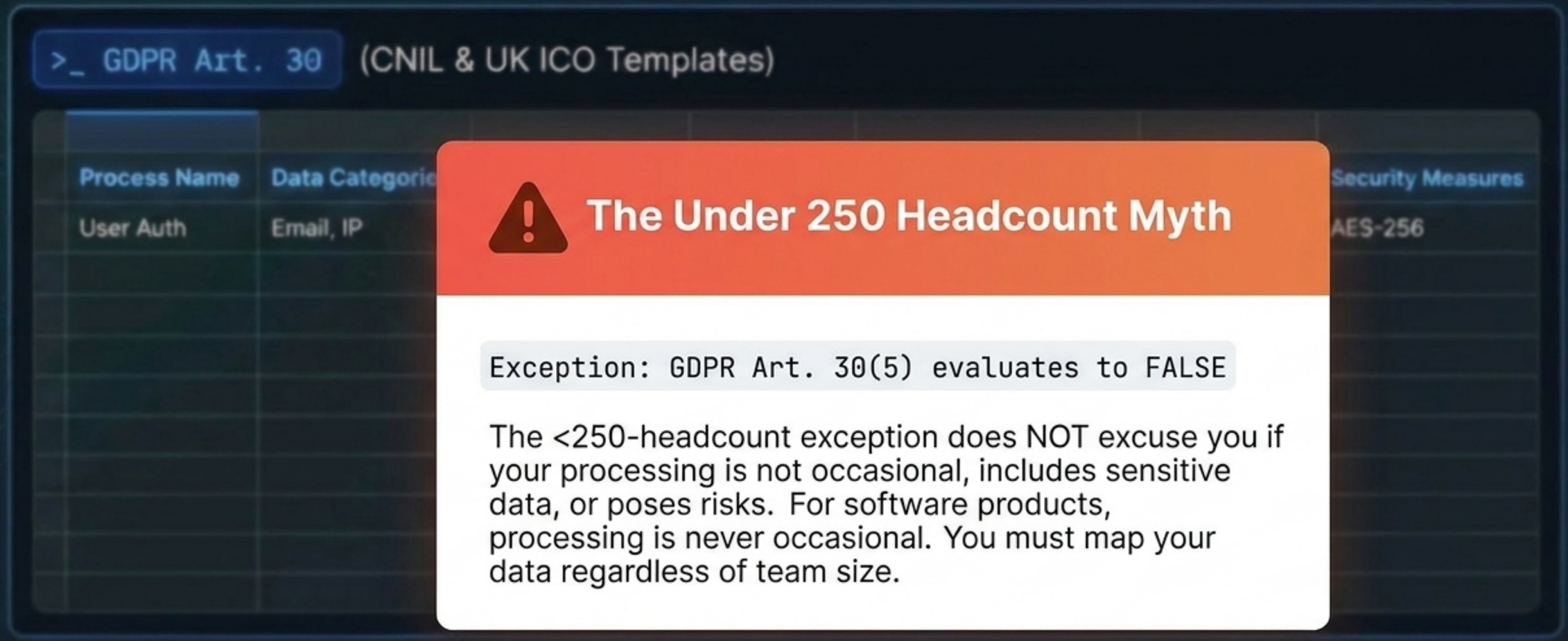
Habit 1: Keep a living, pragmatic data map.

`>_ GDPR Art. 30` (CNIL & UK ICO Templates)

Process Name	Data Categories	Purpose	Legal Basis	Retention / TTL	Recipients	Security Measures
User Auth	Email, IP	Service Delivery	Contract	Account Life + 30 days	AWS, Stripe	AES-256

Gemini Notebook

Habit 1: Keep a living, pragmatic data map.



Gemini Notebook

Panel A: 1-Month DSARs



Data Export/Delete

You have 30 days to retrieve or delete user data upon request. A messy data map means weeks of manual querying. A clean map takes minutes.

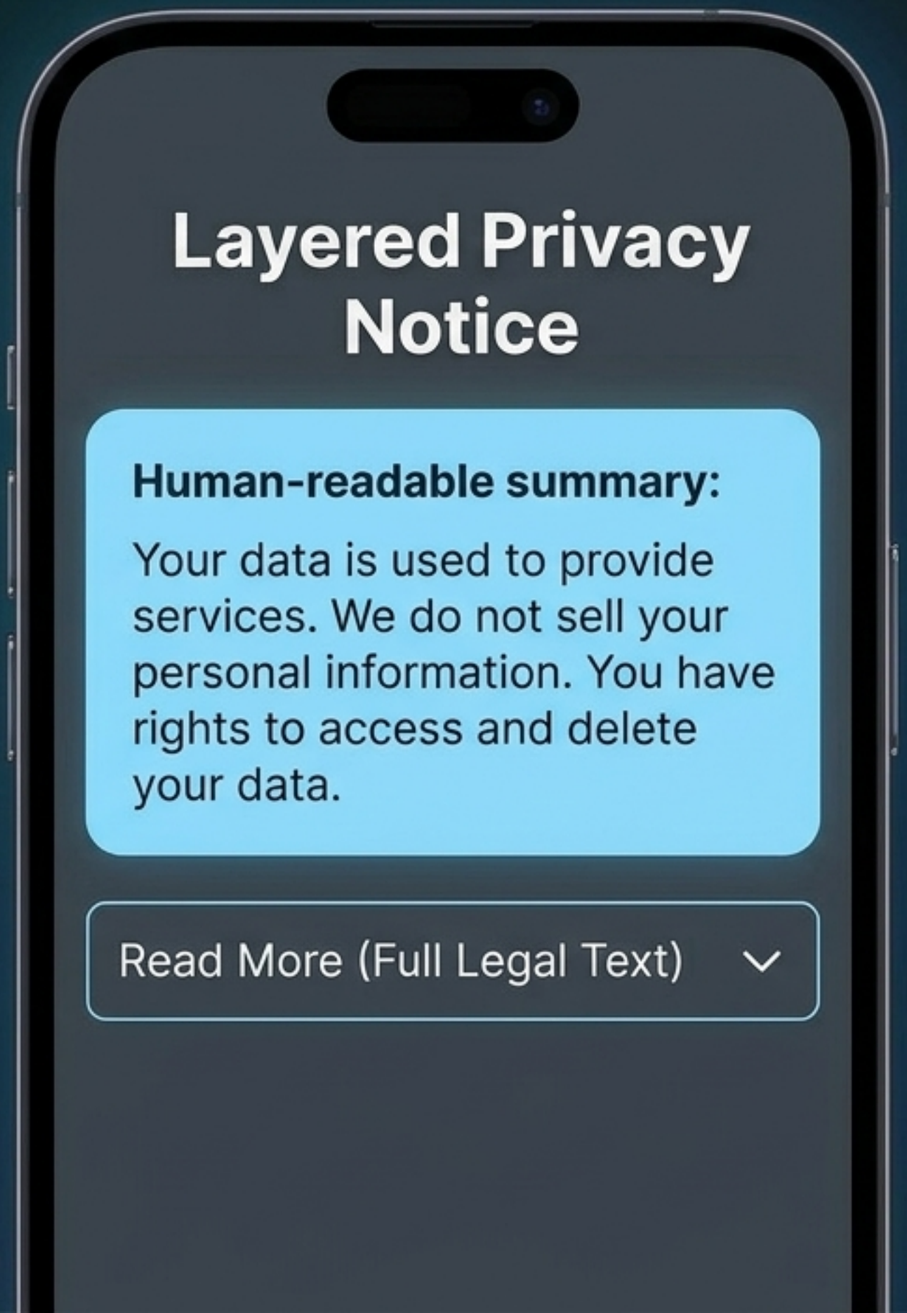
Panel B: Art. 32 Security & TTLs

>_ GDPR Art. 32



Time-To-Live (TTL) automated deletion and encryption are not just good architecture—they are statutory requirements.

Gemini Notebook



Habit 2: Write for humans, structure for compliance.

Utilize WP260 rev.01 guidelines and the ICO Privacy Notice Generator to build ICO Privacy Notice Generator to build layered notices. Stop burying users in walls of legalese.

`>_ GDPR Arts. 12-14`

Gemini Notebook

Match Codebase to CCPA Disclosures

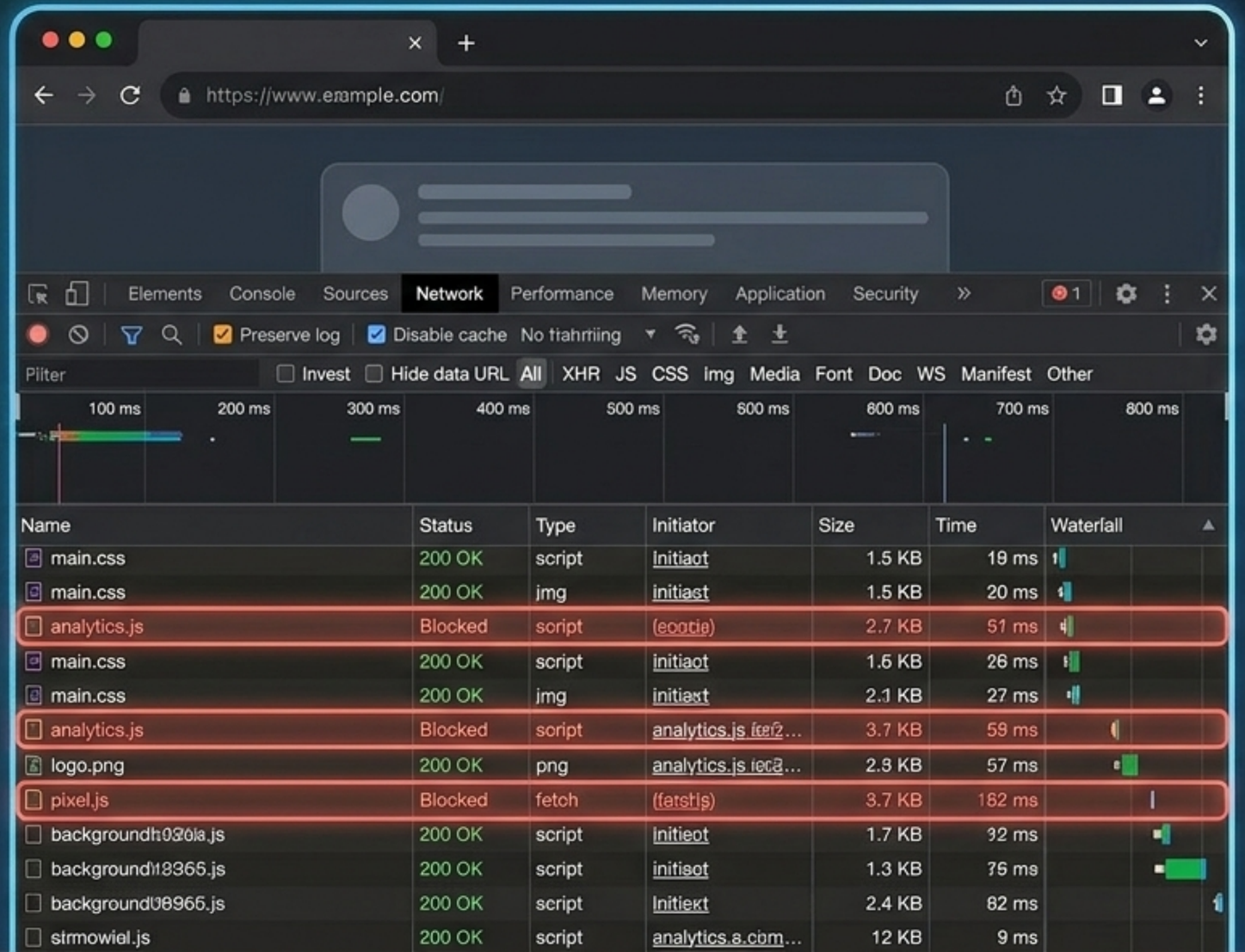
Your disclosures must compile against your actual codebase. Do not copy-paste competitor policies.

Codebase Reality	CCPA Disclosure Requirement
`analytics.track('Location', { precise: true })`	Must clearly state the right to know, delete, correct, limit sensitive info, and opt-out of sale/sharing.

`>_ CCPA § 1798.100 / § 1798.135`

Gemini Notebook

Habit 3: Verify trackers in DevTools pre-launch.



The Absolute Rule:

Zero pre-consent firing. Trackers cannot load before the user explicitly clicks ‘Accept’.

```
>_ ePrivacy Art. 5(3)
```

Gemini Notebook

Symmetric Design (EDPB Cookie Banner Taskforce)

Bad

Accept All

Settings

Good

Accept All | Reject All

'Reject All' must be exactly as easy as 'Accept All'. No dark patterns.

W3C Global Privacy Control (GPC)



Your application must automatically respect the GPC opt-out signal handled via HTTP header.

`>_ GDPR Art. 7(3)`

Gemini Notebook

Habit 4: Never onboard blindly.



Mandatory Checks: Every vendor requires mandatory Data Processing Agreement (DPA) clauses. You must verify their sub-processor lists.

AI Specific: You must actively set LLM ‘zero-training’ flags to protect user data from being absorbed into foundational models.

>_ GDPR Art. 28

>_ EDPB 07/2020

>_ Decision 2021/915

Gemini Notebook

US Data Transfers: DPF vs. SCCs



Data Privacy Framework

Verify active US vendor certification on dataprivacyframework.gov under Decision 2023/1795.

Standard Contractual Clauses

If not on the DPF, you must implement 2021/914 Chapter V SCCs + EDPB 01/2020 encryption checks.

Gemini Notebook

Habit 5: Screen features for mandatory DPIAs.

1. Scoring/profiling
2. Art. 22 automated decisions
3. Systematic monitoring
4. Art. 9 sensitive data
5. Large scale
6. Dataset matching
7. Vulnerable users
8. Innovative/AI tech
9. Preventing rights

Action: If you hit multiple criteria from WP248 rev.01, use official UK ICO or CNIL PIA tools to document your assessment.

>_ GDPR Art. 35

Gemini Notebook

Habit 6: Run the EU AI Act Compliance Checker.



[✓] LITERACY: Ensure Art. 4 AI literacy across your product team.

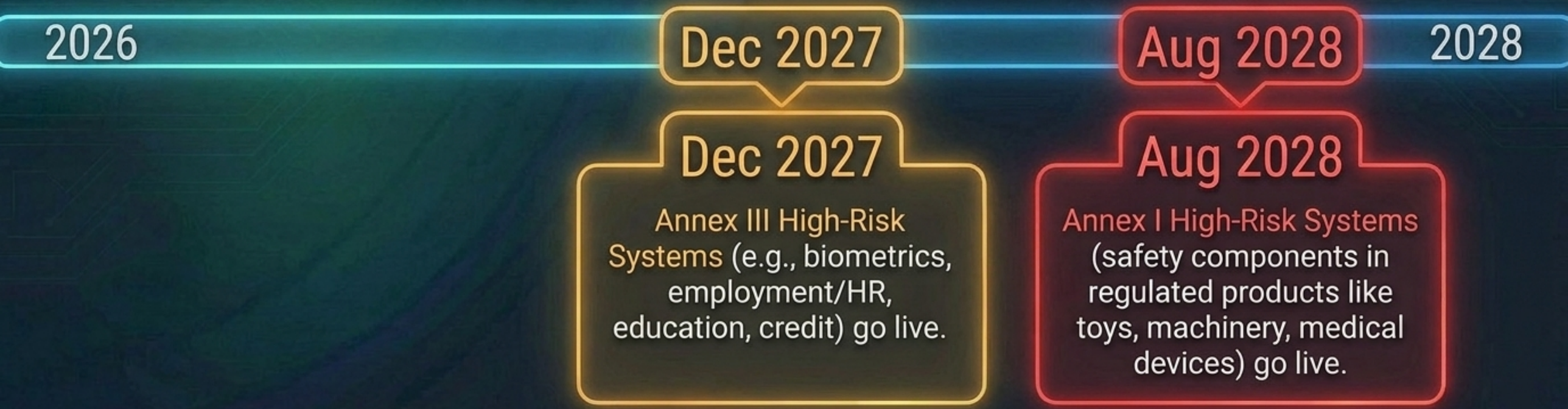
[✓] BANS: Verify absolutely zero Art. 5 Banned Practices (e.g., subliminal manipulation, social scoring, untargeted scraping).

[✓] TRANSPARENCY: Art. 50 requires mandatory UI transparency disclosures for chatbots, deepfakes, and AI-generated content (Live Aug 2026).

Gemini Notebook

AI Act High-Risk Screening Timeline

Screen your product against upcoming high-risk classifications now to avoid forced architecture rewrites later.



Gemini Notebook

The Scenario: A Friday Afternoon Launch.



The Product:
A B2B/prosumer SaaS platform launching a new LLM-powered assistant.

The Goal:
Pass the 6 checklist gates in one afternoon before pushing the final commit to production.

Gemini Notebook

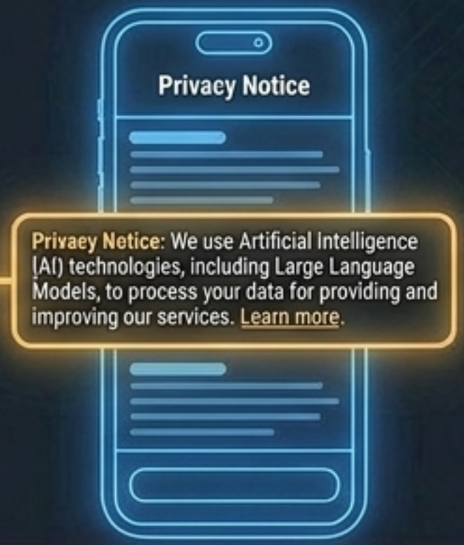
1 Gate 1 (Map)

PM adds ‘LLM Prompt History’ to the ROPA spreadsheet. Sets database TTL to 30 days.

Data Subject Category	Data Category	Processing Purpose	Legal Basis	Retention Period
Users	LLM Prompt History	Service Improvement, Analytics	Legitimate Interest	30 Days

2 Gate 2 (Notice)

PM updates the layered privacy notice UI to explicitly disclose AI usage.



3 Gate 3 (Consent)

Dev realizes analytics fire early. Moves script to trigger after “Accept All”. Configures Sec-GPC: 1 listener.

```
...
...
if (navigator.globalPrivacyControl === "1" || navigator.gpc === "1") {
  // Sec-GPC: 1 listener configured
}

// Analytics script moved to execute after consent
...
```

Gemini Notebook

4

Gate 4 (Vendors)

Team checks OpenAI on dataprivacyframework.gov. Dev toggles “Zero Data Training” via API settings to protect user prompts.



5

Gate 5 (DPIA)

Innovative tech used, but no sensitive data or legal effects. Documented in ICO PIA tool; full DPIA deemed unnecessary.



6

Gate 6 (AI Act)

Dev adds a visible ‘You are chatting with an AI’ disclosure to the chat UI to satisfy Art. 50 (Live Aug 2026).



Status: Ready for Launch.

Gemini Notebook

DIY Startup Hygiene vs. Mandatory Escalation

Green Zone (DIY Hygiene)

- ROPA mapping
- Basic consent UI & GPC
- Routine vendor DPA checks
- Database TTLs
- Standard privacy notices

Engineers and PMs can responsibly maintain this.

Red Zone (Mandatory Escalation)

Triggers where you MUST engage:

- A qualified privacy/AI lawyer
- An external/mandatory Art. 37 DPO
- Regulator consultation (Art. 36)

Stop building. Call for backup.

Gemini Notebook

Escalation Triggers (The Red Lines)



Data Types

Processing Art. 9 health/biometrics or COPPA/ Art. 8 children's data.



AI & Logic

Annex III/I high-risk AI, or Art. 22 automated credit/hiring/legal decisions.



Business Models

Web-scraping/model training on PII, adtech, or data-broker models.



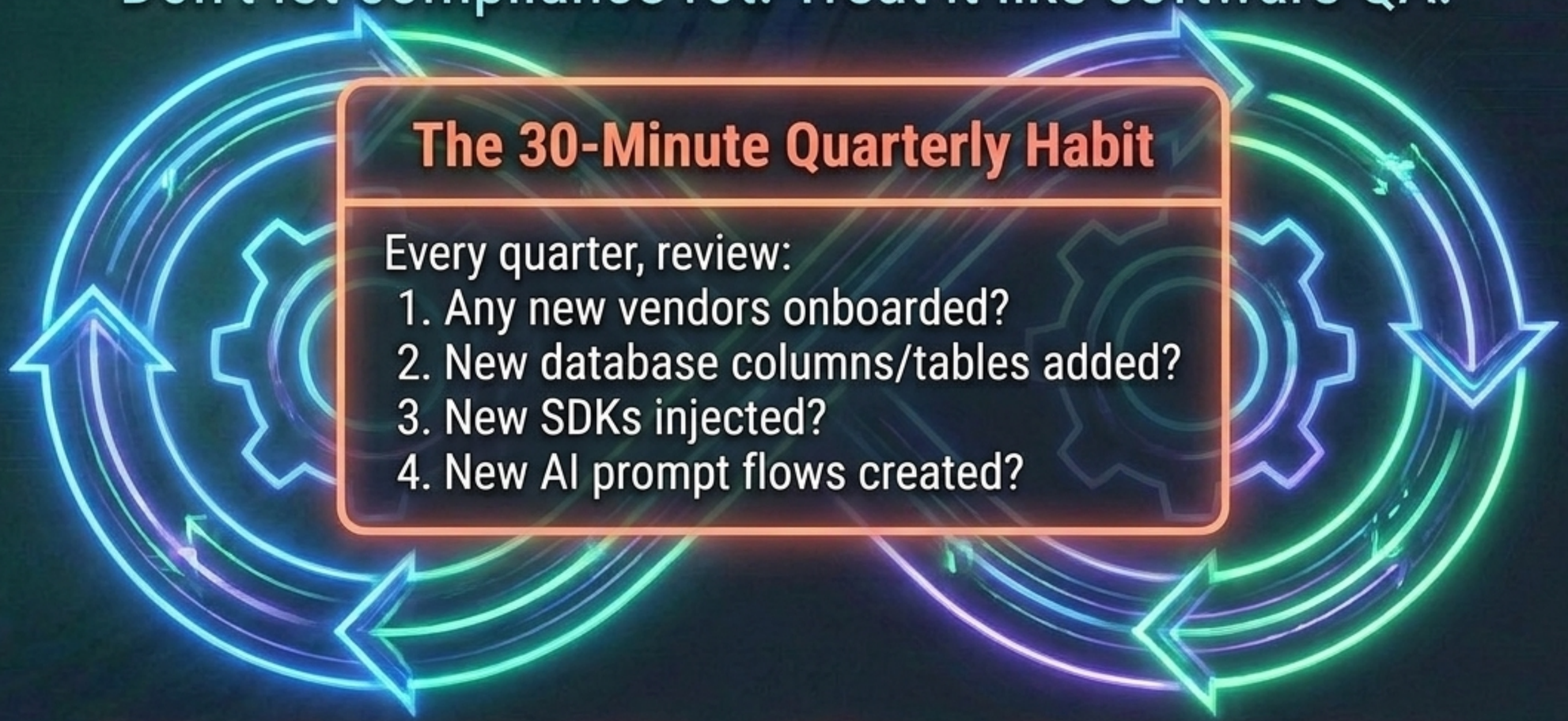
Emergencies

An active 72-hour Art. 33 data breach. **DO NOT DIY A BREACH.**

Gemini Notebook

Keeping Compliance Alive Post-Launch

Don’t let compliance rot. Treat it like software QA.



The 30-Minute Quarterly Habit

Every quarter, review:

1. Any new vendors onboarded?
2. New database columns/tables added?
3. New SDKs injected?
4. New AI prompt flows created?

Action: Update the ROPA and Privacy Notice accordingly.

Gemini Notebook

Official Free Toolkits & Regulatory Sandboxes

You don’t need expensive software for baseline hygiene. Use the official free tools:

- [+] CNIL PIA Tool & Developer Guide
- [+] UK ICO SME Web Hub & Notice Generator
- [+] EU AI Act Compliance Checker
- [+] Art. 57 SME AI Regulatory Sandboxes
  Test innovative AI in a safe regulatory environment before full launch.

Gemini Notebook

```
>_ ./Launch-Protocol.sh --execute
[OK] Map it.
[OK] Disclose it.
[OK] Verify consent.
[OK] Check your vendors.
[OK] Screen for high risks.
[OK] Know your red lines.

Execution Status: Process completed successfully.
```

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

Gemini Notebook