> execute episode_01.sh

Privacy & AI Law — S06E01: GDPR Fundamentals for Product & Engineering Teams

Translating European data protection statutes into product architecture and engineering workflows.

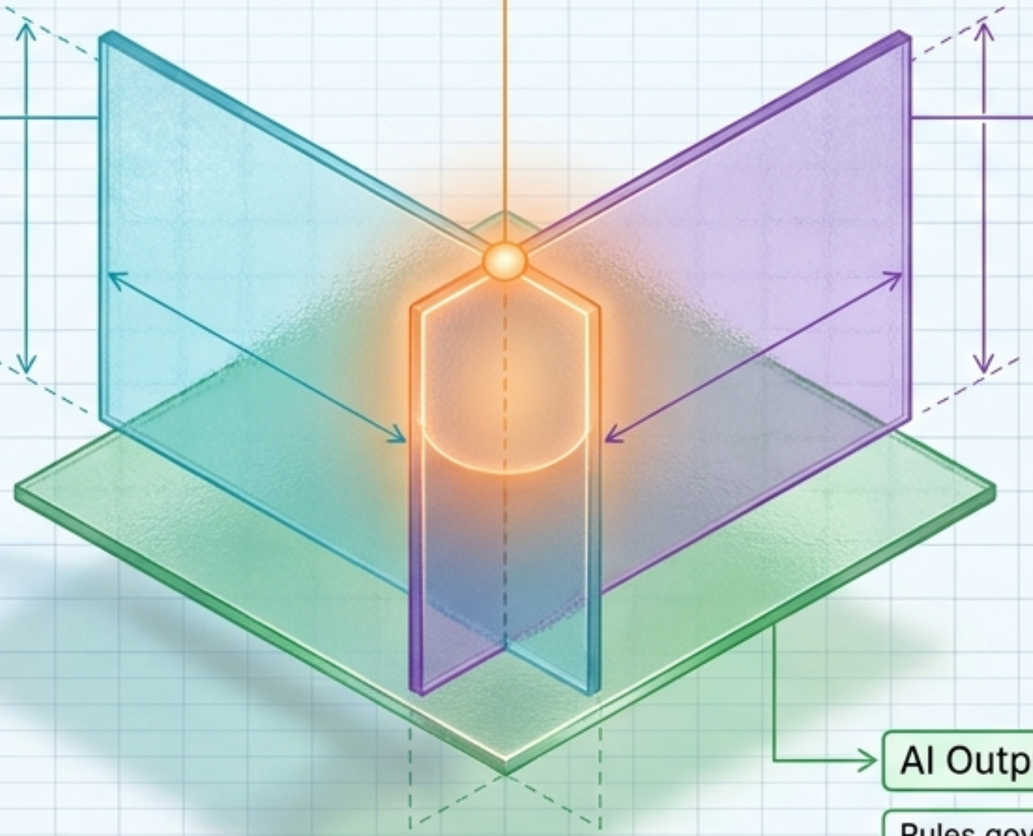
[Founders] [Product Managers] [Developers] [Marketers]

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

Gemini Notebook

The Synthesis

The overlapping mesh where modern software operates.



Privacy Data (GDPR)

Rules governing identifiable human information.

Device & Platform (DMA/DSA)

Rules governing market fairness, algorithmic transparency, and systemic platform risks.

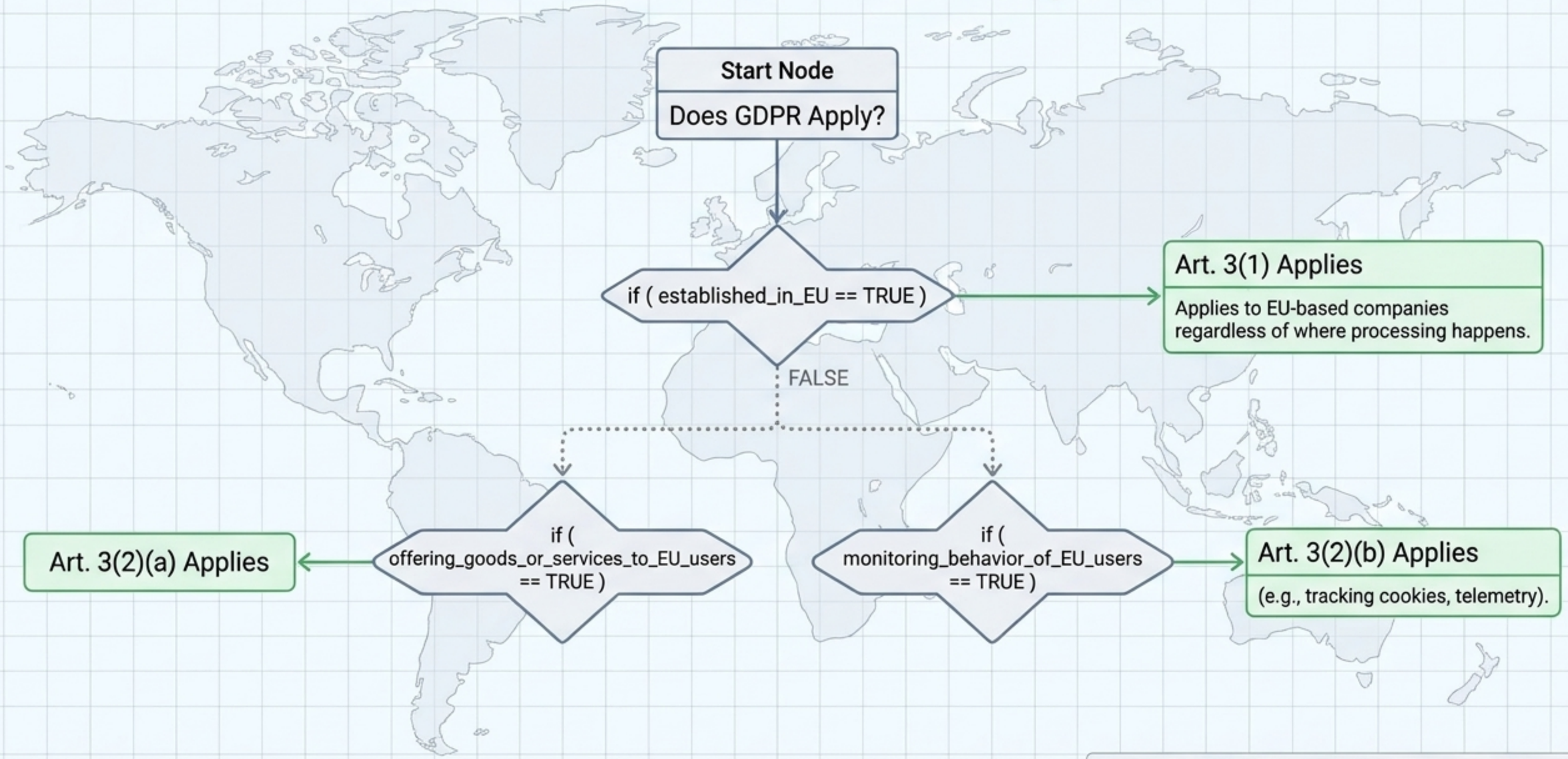
AI Output (AI Act)

Rules governing model risk, training transparency, and automated decision limits.

Modern product compliance requires navigating the overlapping mesh of privacy, device, and AI laws simultaneously.

Gemini Notebook

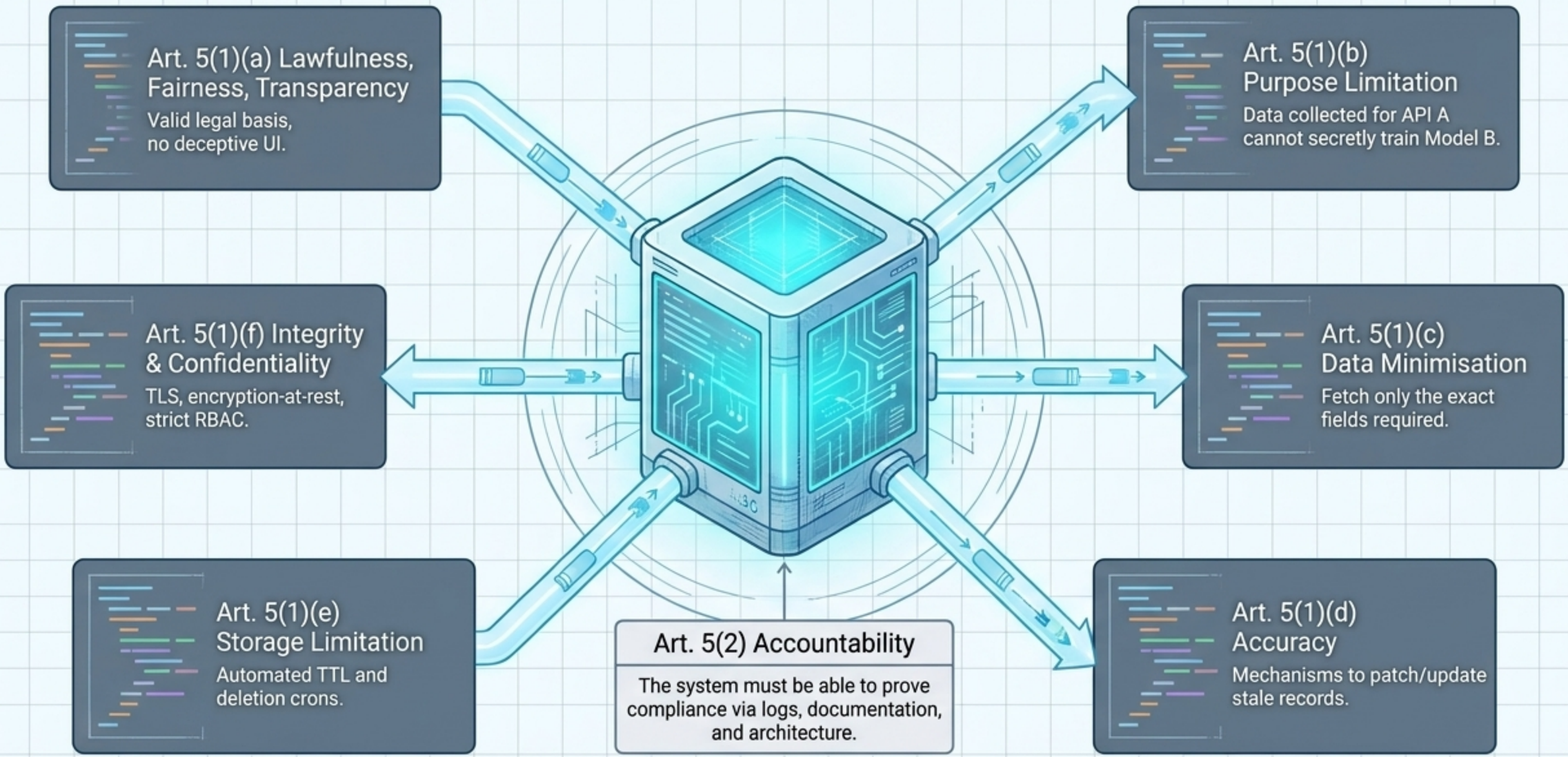
The Global Reach: Territorial Scope (Art. 3)



Source: EDPB Guidelines 3/2018 on territorial scope.

Gemini Notebook

GDPR Principles: Accountability & Core Tenets (Art. 5)



Gemini Notebook

The Controller (Art. 4(7))

Determines the 'Why' and 'How'. The architect of the processing.

Attributes:

- Permissions: Read/Write/Delete/Determine Purpose
- Liability: Primary target for regulatory fines and user requests.

The Processor (Art. 4(8))

Acts strictly on documented instructions. The cloud host, the email sender, the analytics engine.

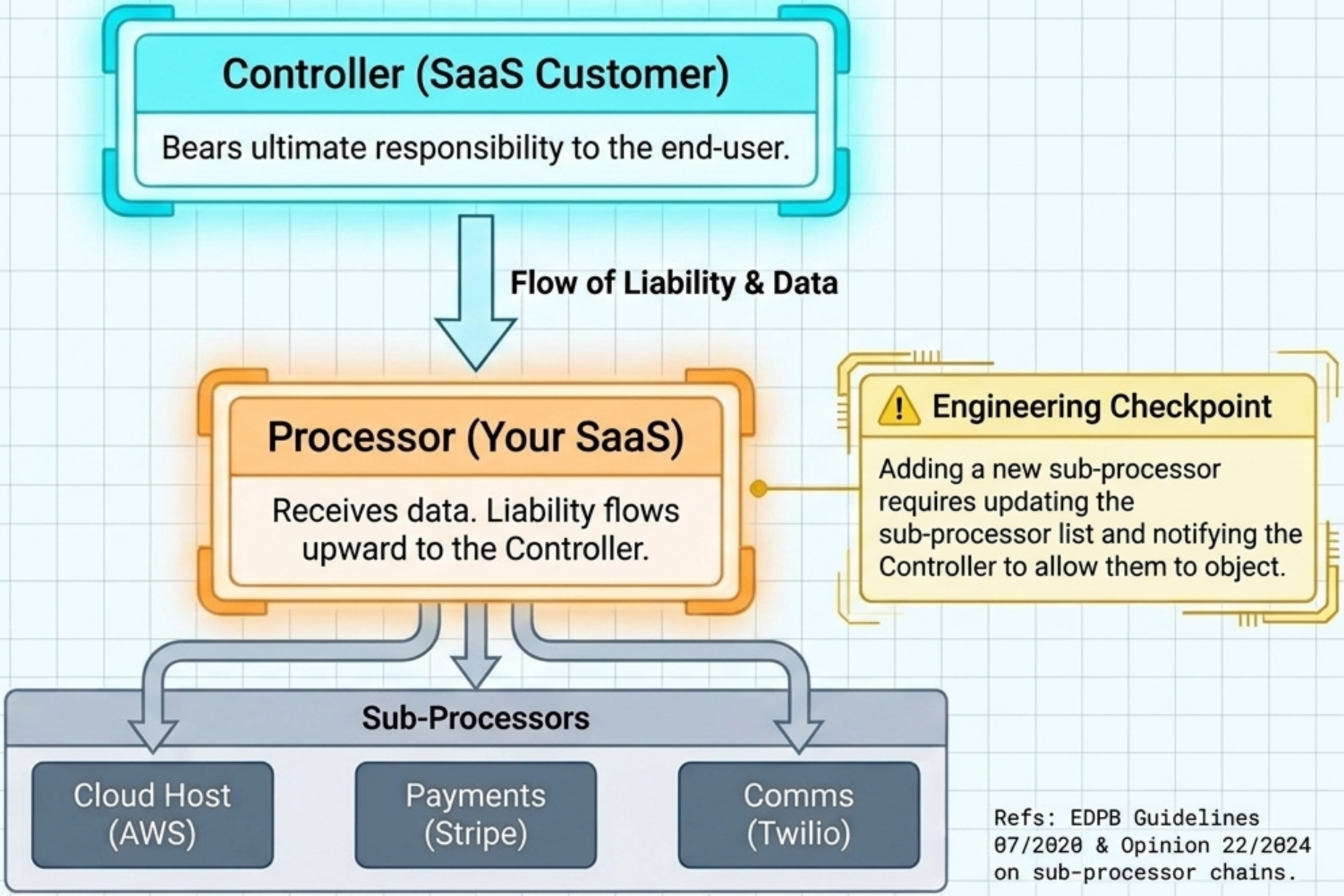
Attributes:

- Permissions: Execute only.
- Limitation: Cannot use data for their own independent purposes.

Joint Controllers (Art. 26)

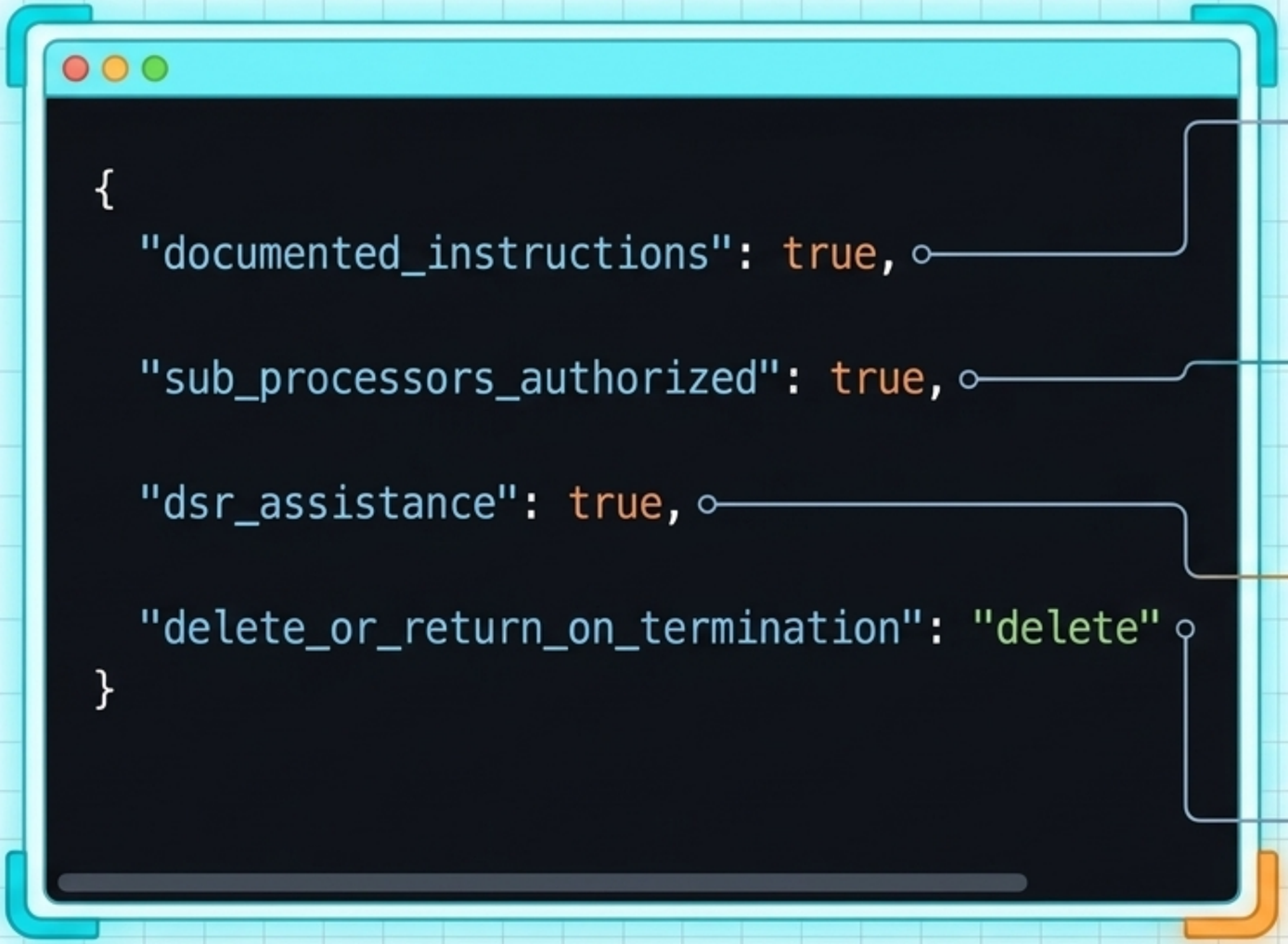
When two entities mutually determine the purpose (e.g., co-branded platforms sharing a unified database).

Gemini Notebook



Gemini Notebook

The Art. 28 Data Processing Agreement (DPA)



Requirement: Process data only as directed. If an instruction breaks the law, throw an exception and notify the Controller.

Requirement: Flow down the exact same Art. 28 obligations to your own vendors.

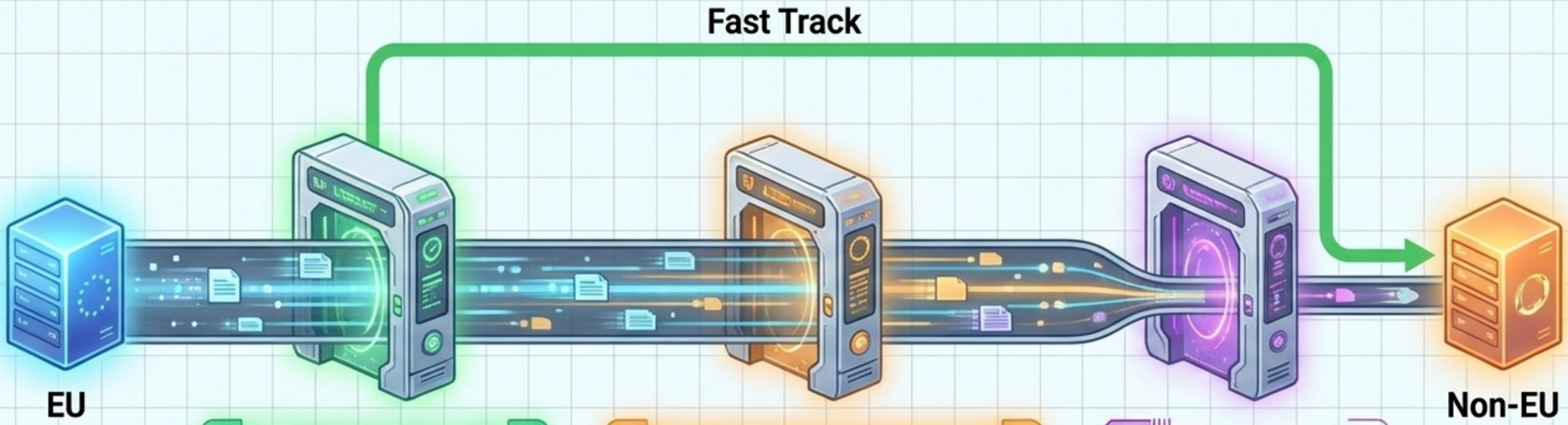
Requirement: Expose APIs or tooling so the Controller can fulfill user data requests.

Requirement: Hard-delete all tenant data upon contract end, overriding standard retention policies.

Ref: Commission Decision 2021/915 (Mandatory clauses)

Gemini Notebook

Chapter V: International Transfer Mechanisms



Art. 45 Adequacy Decision

The EU Commission declares the destination safe.

Current Focus: EU-US Data Privacy Framework (Decision 2023/1795). Certified US companies bypass Checkpoint 2.

Art. 46 Standard Contractual Clauses (SCCs)

Required if Adequacy doesn't apply.

Implementation: Commission Decision 2021/914. Modular contracts (Controller-to-Processor, Processor-to-Processor) legally binding the importer to EU standards.

Art. 49 Derogations

Subtext: One-off emergency transfers (rare for scalable SaaS).

Ref: GDPR Chapter V, EDPB Guidelines.

Gemini Notebook

GDPR Legal Bases: Consent vs. Contract Necessity

Consent (Art. 6(1)(a) & Art. 7)	Contract Necessity (Art. 6(1)(b))
Mechanics: Requires clear, affirmative action. Pre-ticked boxes are void. Must be as easy to withdraw as it was to give.	**Mechanics:** Objectively necessary to deliver the core service promised to the user.
SaaS Example: Optional marketing newsletters, tracking cookies.	**SaaS Example:** Processing a credit card for a subscription, routing an email in a messaging app.
Trap: Using consent for core service data; if the user withdraws consent, the service breaks.	**Trap:** Stretching ‘contract’ to cover analytics or personalization. Scope is strictly narrow.

Ref Tag: EDPB 05/2020

Ref Tag: EDPB 2/2019

Gemini Notebook

GDPR Legal Bases: Specialized & Less Common

Legal Obligation (Art. 6(1)(c))

- **Mechanics:** Processing dictated by EU or Member State law.
- **SaaS Example:** Retaining billing records for statutory tax audits; responding to a valid court order.

Vital Interests (Art. 6(1)(d))

- **Mechanics:** Life-or-death situations.
- **SaaS Example:** Emergency medical routing (Extremely rare for standard B2B/B2C SaaS).

Public Task (Art. 6(1)(e))

- **Mechanics:** Processing carried out in the public interest or official authority.
- **SaaS Example:** University research software, government civic tech.

Ref: GDPR Articles 6(1)(c), 6(1)(d), 6(1)(e); EDPB Guidelines

Gemini Notebook

Legitimate Interests (Art. 6(1)(f))

Business Goals  User Rights

The 3-Step LIA Test (per EDPB 1/2024 & UK ICO)

Step 1: Purpose
Is there a clear, legitimate business interest? (e.g., Fraud prevention, network security).

→

Step 2: Necessity
Is this specific data processing necessary to achieve that goal? (Can it be done with less data?).

→

Step 3: Balancing
Does the processing override the user's fundamental rights, freedoms, or reasonable expectations?

User Rights Impact: Triggers the Right to Object (Art. 21). If a user objects, processing must pause unless compelling grounds are proven.

Ref: GDPR Article 6(1)(f); EDPB Guidelines; UK ICO LIA

Gemini Notebook

Transparency (Arts. 12–14) & **Right of Access** (Art. 15)

Transparency (Arts. 12–14)

Operationalizing Layered Notices
(WP260 rev.01)

- **Layer 1:** In-app contextual tooltip (What are we collecting right now?)
- **Layer 2:** The full, comprehensive Privacy Policy.

Right of Access (Art. 15)



- **Engineering Spec:** Must export a copy of the user's personal data undergoing processing.
- **The SLA Limit:** System must generate and deliver this export within One Month (EDPB 01/2022).
- **Subtext:** Hard deadline requires automated database querying, not manual SQL pulls.

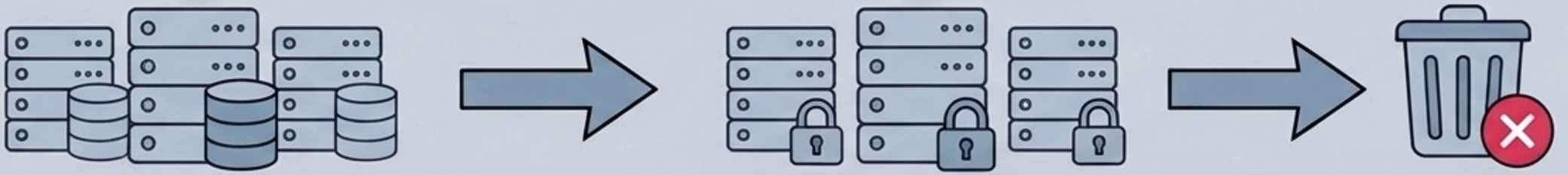
Ref: GDPR Articles 12–15; WP260 rev.01; EDPB 01/2022 Guidelines

Gemini Notebook

Database Lifecycle & User Rights Interventions (Arts. 16, 17, 20)

Right to Rectification (Art. 16) – UI mechanisms allowing users to patch incorrect data payloads.

Art. 17 Erasure in Backups (UK ICO)



Active Live Tables → **Immutable Backup Storage** → **Hard Deletion**

- **Art. 17 Erasure** – Immediate hard delete or irreversible anonymization.

- Data in immutable backups can remain temporarily if put "beyond use," but must be deleted upon the next restoration/overwrite cycle.

Right to Portability (Art. 20). Structured output requirement. User data must be downloadable in a machine-readable format (e.g., standard .json or .csv).

Ref: GDPR Articles 16, 17, 20; UK ICO Guidelines on Erasure; EDPB Guidelines

Gemini Notebook

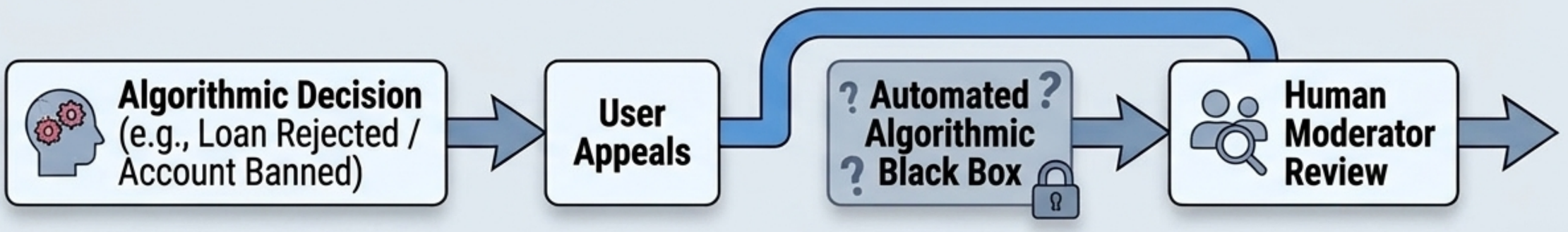
Right to Object (Art. 21)

Direct Marketing Opt-Out OFF

Requires a frictionless opt-out switch, particularly for direct marketing (which is an absolute right).

Automated Decision Limits (Art. 22)

The Rule: Users have the right not to be subject to a decision based solely on automated processing (including profiling) which produces legal or similarly significant effects.



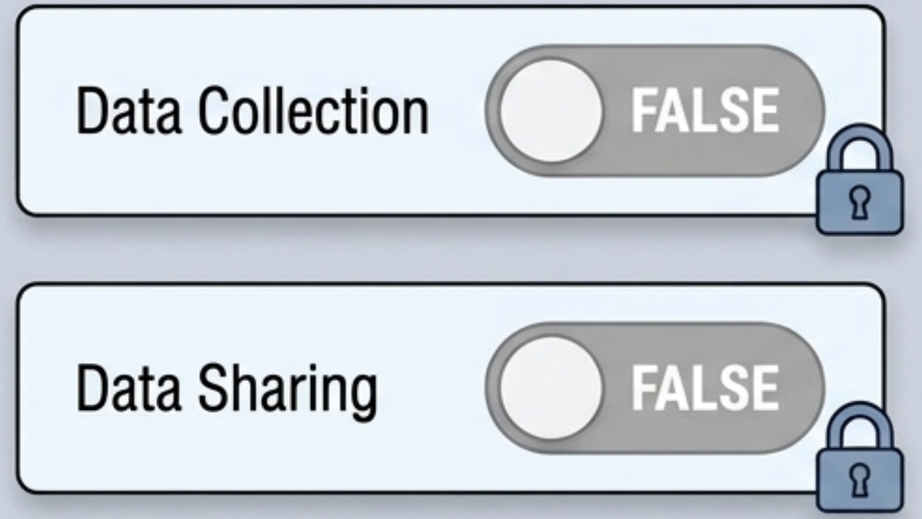
The Engineering Fix: Design a Human-in-the-Loop architecture.

Gemini Notebook

Privacy by Design & Default (Art. 25) **& Security Baselines** (Art. 32)

Privacy by Design & Default (Art. 25)

System variables must initialize to the most privacy-protective state. Opt-in, **never** pre-ticked opt-out (EDPB 4/2019).



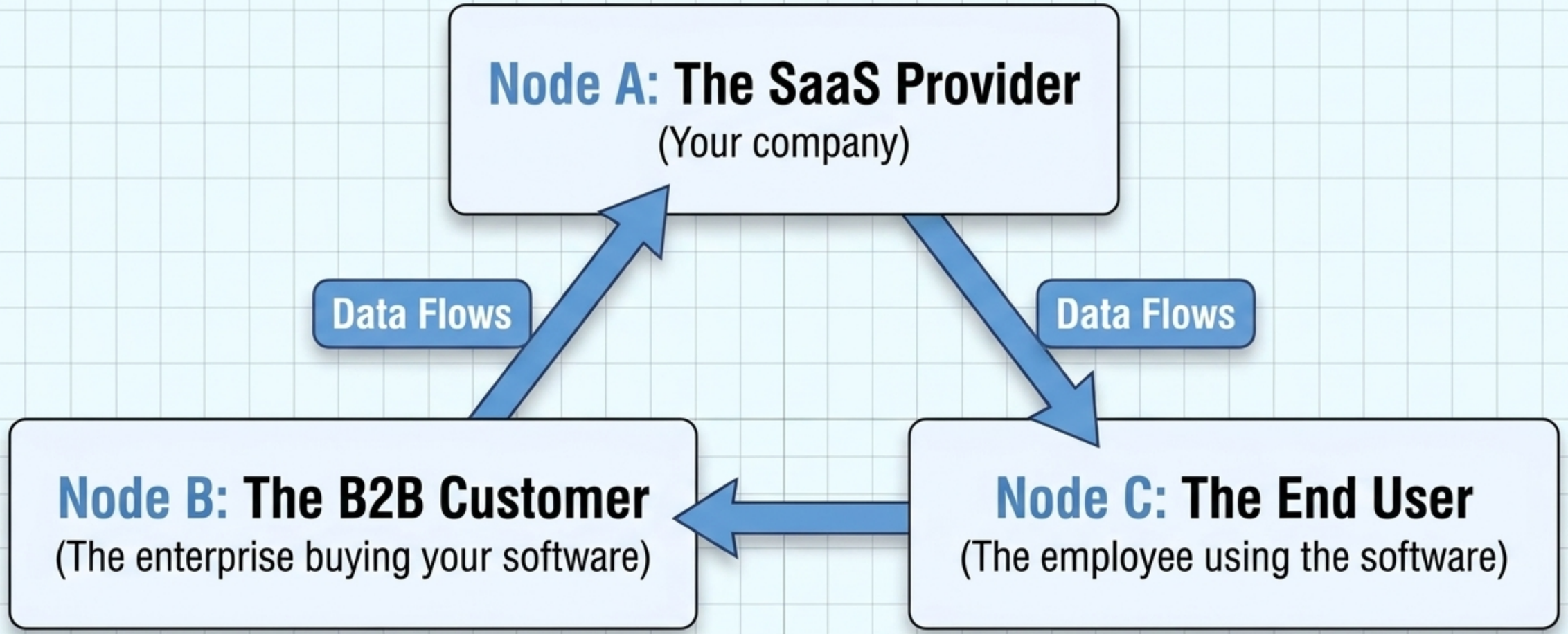
Security Baselines (Art. 32)

Implementing **CNIL** baselines:

- **Encryption** in transit (TLS 1.3) and at rest (AES-256).
- **Strict RBAC** (Role-Based Access Control) to limit internal employee access.
- **Pseudonymization** (separating PII identifiers from the main analytical data payload).

Ref: GDPR Articles 25, 32; EDPB Guidelines on Data Protection by Design and Default; CNIL Security Recommendations.

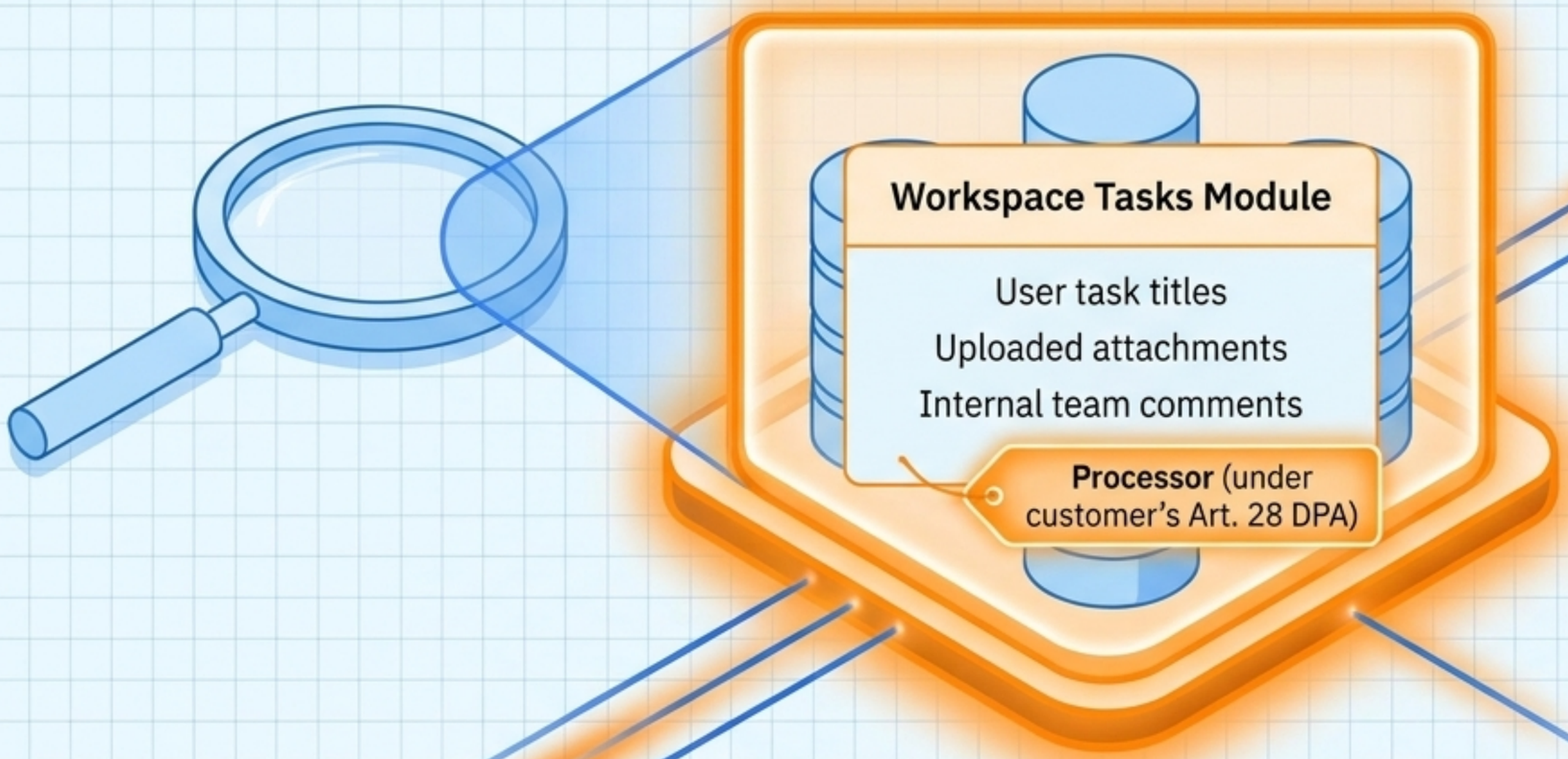
Gemini Notebook



Scenario: A B2B2C Project Management SaaS. The next two slides will zoom in on specific modules within this architecture to determine legal roles.

Gemini Notebook

SaaS as a Processor (The Workspace)



Operational Reality

- The SaaS provider does not determine the purpose of this data.
- If a customer says "delete this workspace," the SaaS provider runs the DROP TABLE command without asking questions.
- The SaaS cannot mine this data to train its own proprietary AI models without explicit DPA authorization.

Gemini Notebook

SaaS as an Independent Controller (The Business)



Billing & Subscriptions

Processing admin credit cards.

Lawful basis: Contract (Art. 6(1)(b)) & Legal (Art. 6(1)(c)) for tax retention.

Security & Audit Logging

Tracking IP addresses to prevent DDoS or credential stuffing.

Lawful basis: Legitimate Interests (Art. 6(1)(f) LIA).

Product Newsletter

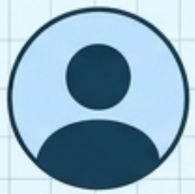
E-mailing users feature updates.

Lawful basis: Consent (Art. 6(1)(a)).

Independent Controller

Gemini Notebook

Handling DSRs in B2B2C Environments



Trigger: Art. 17
“Delete My Account”

API Gateway

Controller Data

SaaS company’s marketing lists and direct billing info.

System executes immediate hard delete or anonymization.

Processor Data

The user’s project tasks and team comments.

System forwards the request to the B2B Customer (the Controller) **OR** handles it via a pre-programmed API endpoint defined in the DPA instructions (e.g., anonymizing the user’s name but keeping the task for team continuity).

Gemini Notebook

High-Risk Features & Mandatory DPIAs (Art. 35)

Data Protection Impact Assessments (DPIAs) are mandatory before shipping features that pose high risks to user rights.



Screening Criteria (If a feature triggers 2 or more, flag for a DPIA):

- [x] 1. Evaluation/Scoring (profiling).
- [x] 2. Automated decision-making with legal effect.
- [x] 3. Systematic monitoring.
- [x] 4. Sensitive data (Special Categories Art. 9/10).
- [x] 5. Data processed on a large scale.
- [x] 6. Matching or combining datasets.
- [x] 7. Data concerning vulnerable subjects.
- [x] 8. Innovative use of new tech (e.g., GenAI).
- [x] 9. Blocking users from a service/contract.

Gemini Notebook

Breach Logging vs. Notification (Arts. 33–34)



Event: Security Incident Detected

Internal Logging
Art. 33 requires documenting all breaches, even minor ones.

If (Risk to Users == TRUE)

TRUE

Supervisory Notification (Art. 33)
Must notify the DPA within 72 hours.
Case Study: Misconfigured cloud bucket exposes emails (EDPB Guidelines 9/2022).

If (HIGH Risk to Users == TRUE)

TRUE

User Alerts (Art. 34)
Must notify affected users directly.
Case Study: Ransomware exfiltrates unencrypted passwords and credit cards (EDPB Guidelines 01/2021).

Gemini Notebook

Administrative Fines in Principle (Art. 83)



Tier 1 Defaults

Tier 1 (e.g., Art. 28 Processor contract failures, Art. 33 Breach reporting delays)

Up to €10 Million
OR
2% of global annual turnover, whichever is higher.



Tier 2 Severe

Tier 2 (e.g., Art. 5 Principle violations, Art. 6 Unlawful processing, Art. 44 Illegal transfers)

Up to €20 Million
OR
4% of global annual turnover, whichever is higher.

Context Factor: Fines are calculated based on the EDPB Guidelines 04/2022 framework, assessing intent, mitigation efforts, and the scale of data affected.

Gemini Notebook

Product Team Takeaways: Five Repeatable GDPR Habits

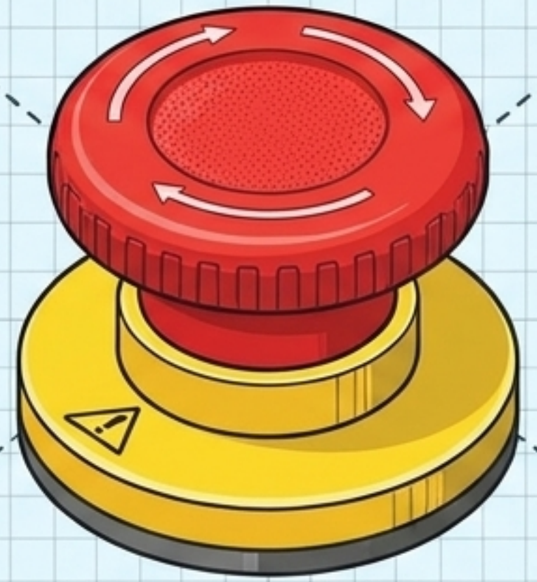
> 1. **map_your_data**: Know exactly what you collect, where it lives, and who it goes to.
> 2. **document_bases**: Hardcode the specific Art. 6 lawful basis into the product spec for every feature.
> 3. **default_to_privacy**: Set initial collection toggles to OFF. Let users opt-in.
> 4. **engineer_deletion**: Build robust TTLs and API endpoints for instant data erasure across live and backup cycles.
> 5. **lock_down_access**: Implement strict RBAC. Engineers shouldn’t have raw access to production PII by default.

Gemini Notebook

Counsel Red Lines: When to Halt and Escalate

Training new AI models on existing user databases.

Expanding product launch into new geographical jurisdictions.



Ingesting large-scale sensitive data (biometrics, health, criminal data under Arts. 9 & 10).

Discovering a live, active data breach exposing user records.

Hit the stop button. Escalate to qualified legal counsel or the designated Data Protection Officer (DPO - Art. 37) before deploying code.

Gemini Notebook

Next Up

S06E02: PII vs. Personal Data — Defining the Boundaries of the Identifiable Human.

Next episode, we explore exactly what constitutes personal data, pseudonymization, and the limits of anonymous analytics under Art. 4(1).

Gemini Notebook