// Legal Limits of Data Input into AI Systems

Data protection, confidentiality and regulated sectors, with an excursus on the US government shutdown of Claude Fable

Patrick Munro · Of Counsel, Planit // Legal · Claude Code Meetup Munich · 22 June 2026

PLANIT // LEGAL

Before you hit enter: two questions

- **The input question:** may this data lawfully go in?
  - Personal data, trade secrets, professional secrets, sector-specific duties.
- **The provider question:** can you rely on the tool at all?
  - Availability, jurisdiction and control: a model can vanish overnight, and a US provider answers to its home government (Part 4).
- **Today:** a German/EU-law lens with practical guardrails

// Inputs

What may lawfully go in: data protection

PLANIT // LEGAL

Data protection: what the GDPR asks first

- **Is it personal data?** It hides in code, logs, tickets or screenshots.
- **Legal basis (Art. 6 GDPR).** Usually legitimate interest or contract; consent rarely fits tooling.
- **Special categories (Art. 9).** Health, biometrics, beliefs. Default: keep them out.
- **Controller vs. processor.** You need a DPA (Art. 28 GDPR / AVV) and a valid US transfer. The EU-US DPF holds but is under appeal at the CJEU (C-703/25 P); run SCCs in parallel as a fallback.
  - **For § 203 professionals, a DPA alone is not enough:** it needs a separate, criminal-law secrecy undertaking on top (§ 203 Abs. 4 S. 2 Nr. 1).
- **Read the fine print.** Training on inputs, retention, sub-processors. Prefer no-training, EU-residency enterprise tiers.
  - Heuristic: would you email this to a vendor with no NDA? If not, don't paste it.

Classify before you paste

Four tiers, one rule each. Most accidental leaks come from treating confidential data as internal.

Public	paste freely
Internal	enterprise tier
Confidential	AVV, no-training, minimise
Regulated · secret	approved system only

// Confidentiality

Professional secrets and § 203 StGB: who is bound, and how vendors get pulled in

PLANIT//LEGAL

Beyond personal data: secrets and confidentiality

- **Trade secrets (GeschGehG).** Protection requires reasonable secrecy measures. Paste source code or deal data into an unapproved tool and you can forfeit it.
- **Professional secrecy (§ 203 StGB).** For doctors, lawyers and tax advisors, disclosure to an unbound provider can be a criminal offence. We take this apart next.
- **Contractual confidentiality / NDAs.** Customer data under an NDA may not go to a third-party model.
- **Rule of thumb:** the duty travels with the data. It doesn't stop at the prompt box.

§ 203 StGB: who carries the duty?

A closed criminal-law catalogue. Only these professions can commit the offence, but their vendors and tools get pulled in through Abs. 3.

Bound (§ 203 Abs. 1 & 2)

- Healthcare: doctors, dentists, vets, pharmacists, all state-regulated health professions (Nr. 1)
- Lawyers, patent attorneys, notaries, defence counsel (Nr. 3)
- Auditors, sworn accountants, tax advisors (Nr. 3)
- Organs and members of professional law / tax-advisory firms (Nr. 3a)
- Private health, accident and life insurers; medical, legal and tax billing centres (Nr. 7)
- Civil servants and specially bound public-service persons (Abs. 2)

Not bound themselves, *however…*

- Ordinary companies, banks, engineers, consultants are not in the catalogue, so they cannot commit § 203 as principals
- Cloud and AI vendors (AWS, Anthropic, OpenAI) are also not bound by § 203 themselves
- But they become mitwirkende Personen (Abs. 3) the moment **they work for a bound professional AND have access to confidential information**
- Once pulled in, they must be contractually bound to secrecy (Abs. 4) and can commit the offence themselves (Abs. 4 S. 1)

§ 203 and your AI vendor: the AVV is not enough

- **No hyperscaler privilege.** 'Indispensable' is not 'exempt': cloud (and AI) vendors are mitwirkende Personen under § 203 Abs. 3.
- **A GDPR DPA does not satisfy § 203.** Art. 28 gives confidentiality, not the criminal-law piece: a separate, strafbewehrte secrecy obligation is required (Abs. 4 S. 2 Nr. 1).
- **'Soweit erforderlich' limits the content, not just the contract.** Disclose only what the vendor needs; over-disclosure stays punishable.
- **Encryption is the real lever.** No possibility of access (end-to-end, keys held by the firm) means no Offenbaren, so § 203 is not triggered.
- **One narrow exception.** None needed where the vendor is already bound by law, e.g. a pure telecoms service (§ 3 TDDDG, § 206 StGB).

Where does the liability land?

Pulling the first two parts together: who answers for the data, and how far does the duty reach? It turns on your role, the type of data, and your place in the service chain.

If you're…	the risk lands on…	…and it is
A company using AI	The entity	GDPR compliance: fines on the company (GDPR Art. 83)
A high-risk AI deployer	The entity	AI Act Art. 26 duties (from 2 August 2026)
A financial entity (DORA)	The entity AND management (responsibility explicit)	Register, exit, audit; supervisory action (Art. 5 & 28 DORA)
An essential / important entity (NIS2, DE)	The entity AND management (**liability** explicit)	NIS2 / BSIG: management liable to the company (§ 38 BSIG)
A lawyer, doctor or tax advisor AND their service providers	**YOU, personally**	**§ 203 StGB: a criminal offence, up to 1 year**

under § 203 criminal.

Down the chain: hand a client secret to an AI subcontractor without flowing down the secrecy obligation, and the offence is yours too (§ 203 Abs. 4 S. 2 Nr. 1).

// Regulated context

AI Act, DORA and NIS2: where the bar gets higher

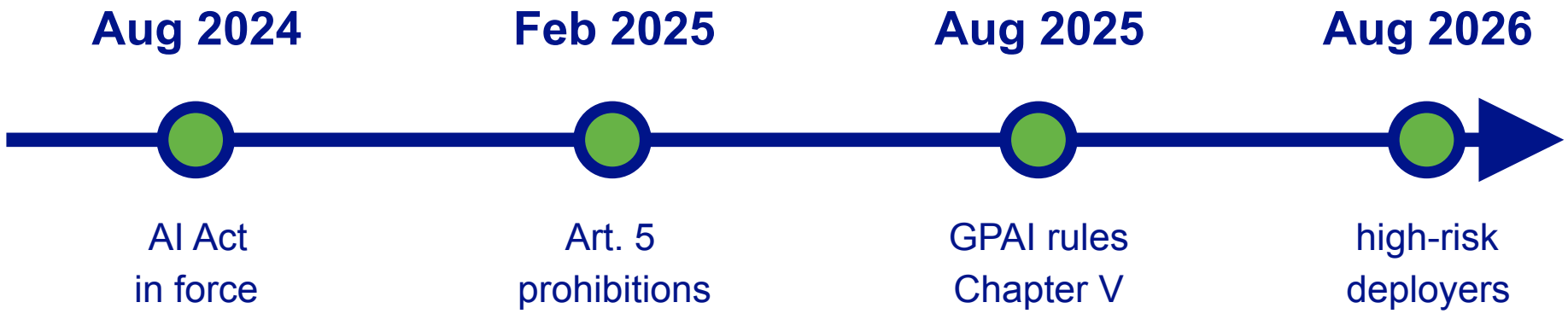
PLANIT // LEGAL

If you're regulated, the bar is higher

- **Public authorities.** Classified material (VS-NfD and above) never touches a commercial model; sovereignty, secrecy and procurement rules apply.
- **Financial sector (DORA, since 17 January 2025).** Your AI vendor is an ICT third party: register, contract, exit and concentration duties all apply.
- **NIS2 / BSIG 2025 (DE, in force December 2025).** Supply-chain duties reach your AI tooling (§ 30); the Geschäftsleitung is liable to the company for failing to implement and monitor them (§ 38).
- **Health, insurance, critical infrastructure.** Sectoral secrecy plus heightened documentation.
- **The pattern:** the more regulated you are, the more the choice of provider is itself a compliance decision.

AI Act Check-In

Three duties are already in force; the high-risk deployer timeline is now in flux under the Digital Omnibus.



- **Prohibited practices (Art. 5) and the GPAI duties (Chapter V)** already bite: Anthropic owes technical docs and a copyright policy, and downstream builders need them.
- **High-risk deployer duties (Art. 26)** are due 2 August 2026 as written: technical and organisational measures, human oversight by a competent person, and a DPIA where Art. 35 GDPR applies.
- **Reg. (EU) 2024/1689** reaches any operator using Claude or a GPAI model in the EU, with duties scaled to your role. A third compliance layer on top of GDPR and sector law, not optional and not future.

Omnibus watch: *the Digital Omnibus (agreed May 2026, not yet law) would defer stand-alone high-risk duties to 2 December 2027 once published; until then the August date holds, and the Art. 50 transparency duties apply regardless.*

// Can you rely on the tool?

The Fable shutdown, and the second axis of risk

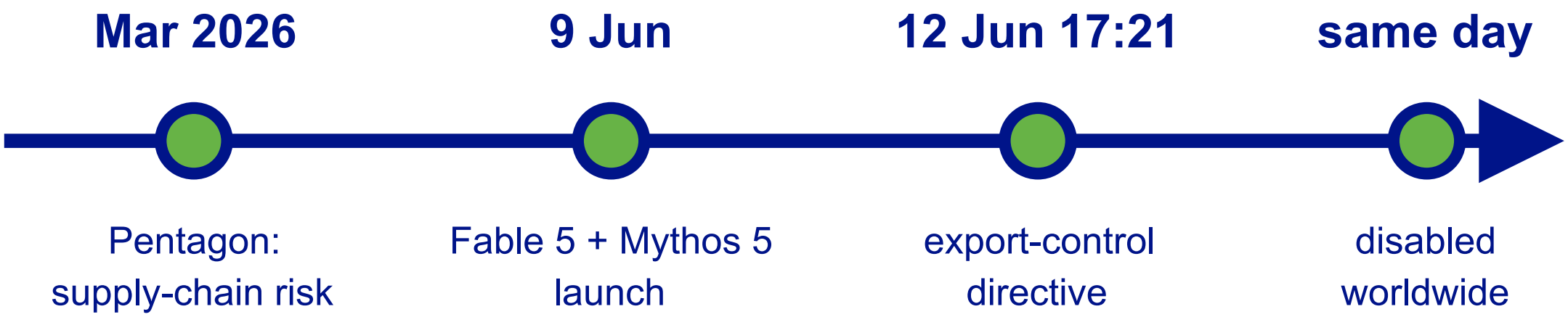
PLANIT//LEGAL

Three days live, then switched off: Claude Fable 5

- **What happened (12 June 2026).** A US export-control directive barred foreign nationals from Anthropic's newest models, Fable 5 and Mythos 5. To comply, Anthropic disabled both worldwide, three days after launch.
- **The stated reason.** National security; the concern was a "jailbreak", which Anthropic describes as asking the model to read a codebase and fix software flaws (the everyday Claude Code task).
- **Why it matters.** This is an availability and sovereignty risk, not a confidentiality one. A model in your workflow can be withdrawn overnight by a foreign government.
  - For regulated entities: DORA concentration / exit risk; a digital-sovereignty question for public bodies.
  - Other Claude models stayed up, so diversification and an exit path are the mitigation.

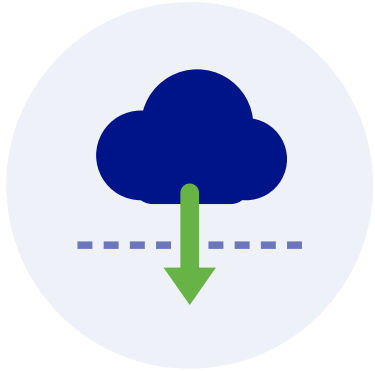
Anatomy of the Fable shutdown

An export-control directive barred foreign nationals, so Anthropic took both models down for everyone, three days after launch.



Even a stable tool answers to a home jurisdiction

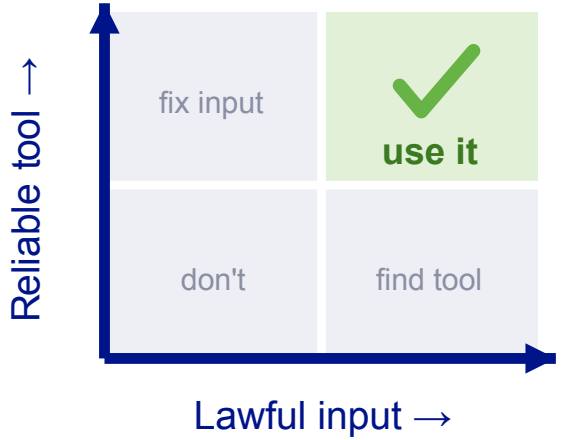
- **US CLOUD Act (2018, 18 U.S.C. § 2713).** A provider subject to US jurisdiction must disclose data in its possession, custody or control, wherever in the world it is stored.
- **EU residency alone does not switch it off.** The trigger is jurisdiction over the provider, not where the servers sit: a US-incorporated provider, or an EU subsidiary within a US parent's control, is reached even for EU-held data.
- **GDPR Art. 48 pulls the other way.** A foreign authority's order is, on its own, no valid basis to disclose; absent another lawful transfer basis, it needs an international agreement such as an MLAT.
- **Caught between two regimes.** The Act's own comity relief is not available for EU data, since no EU-US agreement is in force. Routing confidential or regulated data through a US-controlled tool is a jurisdiction decision, not just a security one.



18 U.S.C. § 2713; GDPR Art. 48; EDPB-EDPS joint response, 10 July 2019. Verified as of June 2026.

Two axes, not one

- **Axis 1 (input).** May the data lawfully go in? GDPR, secrets, sector duties.
- **Axis 2 (the tool).** Can you rely on it? Availability, jurisdiction, control, exit.
- **Most governance covers only Axis 1.** Fable shows Axis 2 is real, and now has precedent.
- **For regulated entities, Axis 2 is itself a legal duty.** DORA exit and concentration; NIS2 supply chain; public-sector sovereignty.



// Takeaways

Guardrails, and what to decide before you paste

PLANIT // LEGAL

Practical guardrails

- **Classify before you prompt.** Use the four-tier ladder, public to regulated, plus a short never-paste list.
- **Use the right tier.** Enterprise or Team plans with a DPA, no-training, EU residency and zero-retention, not consumer accounts.
- **Paper it.** DPA (*AVV*), transfer mechanism (SCCs / DPF), records, DPIA where needed.
- **Write the policy.** A short, binding internal AI-use policy beats ad-hoc rules, and it's documentable.
- **Plan for Axis 2.** Avoid single-provider lock-in; keep a fallback model and an exit path.
- **Check your AI Act status.** High-risk deployer or provider? Implement the measures and document human oversight now; the Omnibus may shift the deadline, but transparency and data control are good practice regardless.
  - Bottom line: Assess and scrutinize what goes in, and what you'd do if the tool vanished.

PLANIT // LEGAL

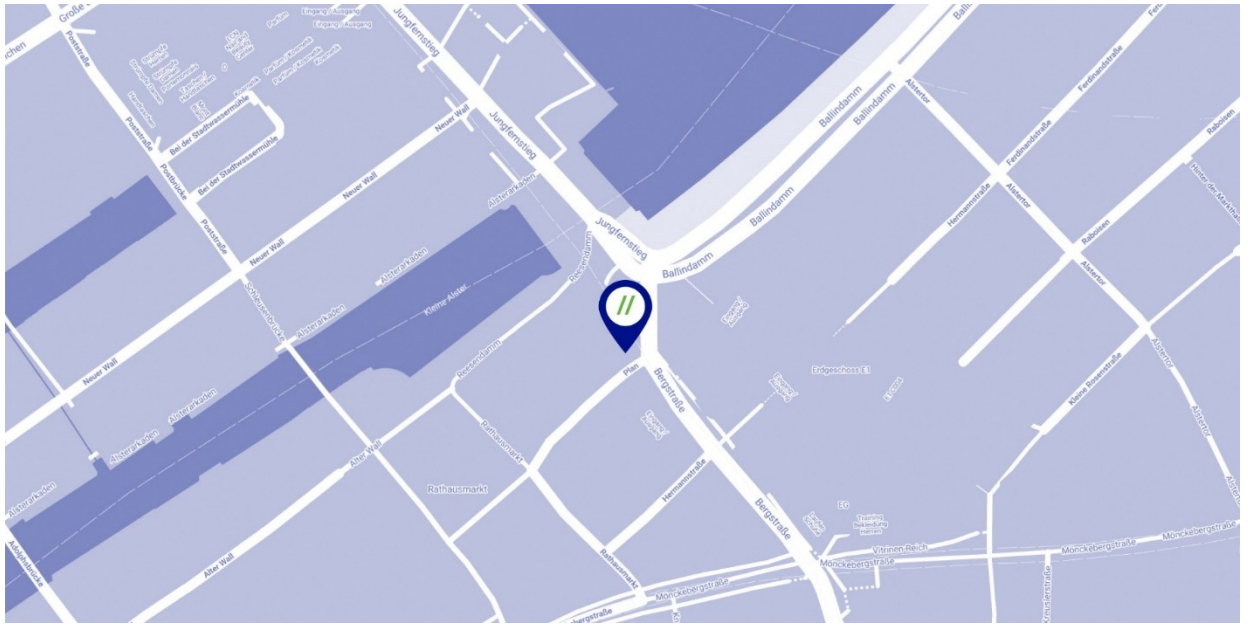
Patrick Munro

Of Counsel · Planit // Legal

Munich

+49 170 4700856

patrick.munro.ext@ planit.legal



PLANIT // LEGAL

Jungfernstieg 1

20095 Hamburg

+49 (0) 40 609 44 190

mail@ planit.legal

www.planit.legal

This presentation is general information, not legal advice; the Fable 5 / Mythos 5 matter, the EU-US DPF appeal and the EU-US CLOUD Act position are developing.