

Sentinel — A Methods & Positioning Note

Christopher I. V. Farmer, LL.M. (University of Worcester) · Independent Researcher · civfarmer@gmail.com

Positioning note; not peer reviewed. Version 1.1, October 2026. Companion to the Sentinel readiness assessor. Law stated as-of 16 October 2026. Decision-support, not legal advice.

DOI: <https://doi.org/10.5281/zenodo.23462152>

Scope note. This note explains what Sentinel is, how it reaches its conclusions, and — just as importantly — what it is *not*. Sentinel is an offline decision-support instrument, not a legal adviser and not an official export-control authority. Every position it takes is dated and labelled; none of it should be relied upon without confirming the current primary sources.

The problem: two legal questions, answered in one pass

Any serious AI or autonomous-system programme has to satisfy two distinct bodies of law that are almost never assessed together. The first asks whether it is **lawful to build and use** the system — its risk tier under the EU AI Act (Regulation (EU) 2024/1689 [2024] OJ L, 2024/1689) and the obligations that tier triggers. The second asks whether it is **lawful to move** the system, its source, its model weights, or its underlying compute across a border — the EU Dual-Use Regulation (Regulation (EU) 2021/821 [2021] OJ L206/1) and the control lists of the Wassenaar Arrangement, one of the regimes its Annex I implements, with US EAR/ITAR exposure layered on top.

In practice these are handled by different teams, different advisers, and different timelines, and the seam between them is exactly where a compliant-looking product becomes an unlawful export — or where an export-cleared item quietly breaches a prohibited-practice rule. Sentinel’s premise is that the two questions draw on almost identical inputs — what the system does, its data and autonomy, its sectors, and the jurisdictions of build and use — and can therefore be answered together, in a single structured pass, early enough to change the design.

The method: a deterministic rules engine

Sentinel is not a model and makes no probabilistic prediction. It is a **deterministic rules engine** — a set of pure functions that map a structured description of a deployment onto the applicable legal categories, so the same description always yields the same classification, reasons and verdict (only the record’s reference number and generation time vary). The engine makes no network calls and runs offline; the hosting site loads analytics only with the visitor’s consent. The AI Act classifier walks Article 5 (prohibited practices), Annex III and Annex

I (high-risk), and Article 50 (transparency obligations), returning exactly one of four tiers — *prohibited*, *high-risk*, *limited-risk*, *minimal-risk* — together with the specific article or annex that fired. A parallel export screen tests the same facts against the Dual-Use Regulation’s Article 4 end-use catch-all and Article 5 cyber-surveillance catch-all, the Annex I control-list categories, and the Wassenaar Category 3/4/5 controls, with an honest, unresolved flag that US EAR or ITAR could bite extraterritorially, raised on the surveillance, intrusion, cryptography, compute and military paths. The two results are combined into a single verdict — *deployable*, *deployable with controls*, *blocked*, or *more information needed* — plus an exportable, audit-ready control record.

Every reason is tagged — and dated

The engine’s defining discipline is that **no reason is left unlabelled**. Every reason line in its classification and export screens carries one of four tags, so the reader can always see where the law ends and the reasoning begins:

Tag	What it means
Legal fact	A statement of what the instrument actually says — the article, annex, or control-list entry.
Assessment	A reasoned application of that law to the described facts — the author’s judgement, not black-letter law.
Verify	A point the user must confirm against current sources before relying on it: a moving date, a US-law overlay, or a fact only the user knows.
Action	A concrete step — screen the end-user, classify the item, obtain the licence, keep the record.

The obligation checklists and control measures that follow the reasons are untagged lists of steps, and the transparency and high-risk application dates appear as timeline lines, flagged in the same way as **legal fact**.

Every position is dated to **October 2026** and pinned to the **Digital Omnibus on AI** (Regulation (EU) 2026/1744 [2026] OJ L, 2026/1744) — the amending Regulation adopted by the European Parliament on 16 June and the Council on 29 June 2026 and signed on 8 July 2026, which moves the high-risk obligations to 2 December 2027 for Annex III systems and to 2 August 2028 for Annex I systems, and inserts two new prohibitions into Article 5(1), points (ba) and (bb), on AI systems that generate or manipulate non-consensual intimate material or child sexual abuse material, applicable from 2 December 2026. The July 2026 version of the tool was written while the Regulation was *adopted but not yet in*

force — awaiting Official-Journal publication — so the lines that depend on it were flagged **verify**, not **legal fact**. That is the whole point of the tagging: the tool refuses to launder a pending date into a settled rule. The Regulation was published in the Official Journal on 24 July 2026 and has been in force since 27 July 2026; the current version flags those lines **legal fact**, and the check that safeguards against the new prohibitions are in place is tagged **action**.

The thesis: regulated by design

Sentinel’s normative claim is that governance is not a disclaimer appended to a finished product but a **design layer built into it** — *regulated by design*. The same engine that classifies the system also names the controls that make the answer defensible: **meaningful human authority** (a real override, pause, and stop authority proportionate to the system’s autonomy — Art 14 / Art 26); **immutable auditability** (tamper-evident event logs, decision provenance, and, where triggered, a Fundamental Rights Impact Assessment under Art 27 or a GDPR DPIA under Art 35); and **export screening wired into the control layer** rather than bolted on at the loading dock. A system built this way is not merely compliant on the day it ships — it can *prove* it was governed, which is the question a regulator or a court actually asks after the fact.

Scope and limits

Sentinel is **decision-support, not legal advice**, and nothing it returns is an **official control classification**. It creates no lawyer–client relationship, binds no authority, and does not substitute for a formal export-control ruling (BIS / BAFA / ECJU) or a qualified legal opinion. It screens export-control exposure, not data-transfer lawfulness: cross-border flows of personal data (under Chapter V of the EU and UK GDPR, or Articles 16 and 17 of the Swiss Federal Act on Data Protection) are outside its scope and need their own assessment. Its outputs are only as good as the description entered; the law moves; and the **verify**-tagged lines mark exactly where the user must consult a primary source or a competent adviser before relying on the result. It is offered as a structured first pass — a way to see both legal questions at once, while the design can still be changed — not as the last word on either.

— Christopher I. V. Farmer, LL.M. (University of Worcester) · Independent Researcher · civfarmer@gmail.com

Suggested citation: Christopher I. V. Farmer, ‘Sentinel — A Methods & Positioning Note’ (positioning note, version 1.1, October 2026) <<https://civfarmer.github.io/publications/sentinel-positioning-note.html>>. <<https://doi.org/10.5281/zenodo.23462152>>. *Licence:* Creative Commons Attribution-NonCommercial 4.0 International (CC BY-NC 4.0). Commercial use needs a licence from the author: civfarmer@gmail.com.