GDPR for Video Surveillance - Compliance Starter

A camera that records people processes personal data. Frame the deployment before you procure. Engineering guidance, not legal advice - confirm specifics with qualified counsel.

Your lawful basis comes first (GDPR Art. 6)

For most private operators the basis is legitimate interests (Art. 6(1)(f)) - a DOCUMENTED three-part test, not a label: (1) Purpose - a real, present, articulated interest (not hypothetical); (2) Necessity - no less intrusive way, only the data the purpose needs; (3) Balancing - your interest not overridden by people's rights and reasonable expectations (gyms, restrooms, restaurants weigh against you). Public authorities -> public task (6(1)(e)); statute-mandated recording -> legal obligation (6(1)(c)); consent (6(1)(a)) rarely works for open-area CCTV.

The GDPR duties, each tied to its article

Duty	What it means for the system	Anchor
Lawful basis	Document it before recording; LIA for legitimate interests	Art. 6
Data minimisation	Only the data the purpose needs; no audio unless required	Art. 5(1)(c)
Storage limitation	Keep a few days; delete automatically	Art. 5(1)(e)
Data-subject rights	Access (+ redact others) & erasure; reply within 1 month	Art. 15/17
Security	Encryption in transit/at rest + access control	Art. 32
Processor & transfers	Written DPA with the cloud VMS; mechanism if data leaves the EEA	Art. 28 / Ch. V
DPIA & records	DPIA before launch for large-scale/biometric; keep the register	Art. 35 / 30

The biometric gate (GDPR Art. 9)

Recording video runs on an Art. 6 basis. Running FACIAL RECOGNITION converts a face into a biometric template (Art. 4(14)) = special-category data (Art. 9), PROHIBITED by default unless an Art. 9(2) exception applies. For commercial surveillance the only realistic exception is explicit consent - and you would need it from EVERYONE in frame, not just enrolled individuals. In open spaces that is usually impossible, so public-space facial recognition is rarely lawful under GDPR. Treat the biometric toggle as a gated decision with its own consent, DPIA, and counsel sign-off.

Tell people: the two-layer notice (Arts. 12-13)

First layer (warning sign at eye level, before the area): purpose of the surveillance, identity & contact of the controller, that rights exist, and where to find more. Second layer (full Art. 13 notice at reception, a website, or a QR code): lawful basis and the interest pursued, retention period, who footage is shared with, whether it leaves the EU, and how to exercise rights. 'CCTV in operation' alone does not meet the standard.

Run before you procure

[ ] Purpose written down per camera (specific, not 'general security'). [ ] Lawful basis chosen + LIA documented. [ ] Facial recognition OFF unless gated with consent + DPIA + counsel. [ ] Two-layer signage drafted. [ ] Retention set to days, deleted automatically. [ ] System can search, export, and redact for access requests. [ ] DPA signed with any cloud/processor; transfer mechanism if data leaves the EEA. [ ] DPIA done before launch; record of processing kept.

This is engineering guidance, not legal advice. The lawful-basis test, the Art. 9 gate, the signage and retention norms, and the fine figures are summarised for planning - confirm the specifics for your jurisdiction with qualified counsel. GDPR fines reach EUR 20M or 4% of global turnover (Art. 83). The EU AI Act adds a layer above GDPR and its dates are in flux (re-verify at use).