Privacy by Design for Surveillance - Starter Guide

A camera pointed at people is a privacy product. Frame the deployment before you procure. Engineering guidance, not legal advice - confirm specifics with counsel.

The decision that matters most: recording video vs running biometrics

Recording identifiable video = personal data (GDPR Art. 4(1)); allowed WITH a lawful basis (Art. 6). Running face recognition = special-category biometric data (Art. 9); PROHIBITED by default unless a narrow exception (e.g. explicit consent) applies. In the US, biometric capture triggers laws like Illinois BIPA: written consent + private right of action ($1,000 / $5,000 per violation). Treat the biometric toggle as a gated, deliberate decision - never a default.

Data-minimisation levers - collect & expose the least that does the job (Art. 5(1)(c), Art. 25(2))

Lever	What it reduces	Anchor
Purpose per camera	Scope of what is recorded at all	Art. 5(1)(b)
Field of view / privacy zones	Scene captured (mask what you don't need)	EDPB 3/2019
Resolution & frame rate	Detail captured beyond the purpose	Art. 5(1)(c)
Disable unneeded analytics	Face recognition / audio data created	EDPB 3/2019
Short retention	How long personal data is kept	Art. 5(1)(e)
Scoped access (need-to-know)	Who can view each person's image	Art. 25(2)

DPIA quick test - do it BEFORE procurement (GDPR Art. 35)

[ ] Systematic monitoring of a publicly accessible area on a large scale? -> DPIA required (Art. 35(3)(c)). [ ] Large-scale biometrics / special-category data? -> DPIA required (Art. 35(3)(b)). [ ] Otherwise likely high risk? -> DPIA (Art. 35(1)). The DPIA shapes the design: purpose, minimisation, the biometric gate, safeguards.

Privacy by design = GDPR Art. 25 (and ISO 31700-1:2023)

Proactive not reactive - privacy as the DEFAULT setting - embedded in design - full functionality (not zero-sum) - end-to-end lifecycle - visible & transparent - user-centric. Art. 25(1): build data-protection principles in at design time. Art. 25(2): by default process only necessary data - amount, extent, storage period, and accessibility.

Privacy posture checklist (run before specifying a system)

[ ] Assume the system handles personal data; design accordingly. [ ] Gate the biometric decision (lawful basis + consent + DPIA). [ ] Minimise by default across every lever above. [ ] Complete the DPIA before procurement and use it to shape the design. [ ] Build masking / redaction into the pipeline. [ ] Get consent & notice right; design to the strictest region you operate in. [ ] Keep footage briefly; scope access to need-to-know; log access & deletion.

This is engineering guidance, not legal advice. The video-vs-biometrics gate, DPIA triggers, and BIPA figures are summarised for planning - confirm the specifics for your jurisdiction with qualified counsel. EU AI Act dates are in flux (re-verify at use).