AI Security Camera + Intelligent Video Analytics — Decision Sheet

1 - The feature catalog (the group decides everything)

Detect	Person/vehicle, intrusion, line-crossing, object-left, PPE, fall. Pipeline: object detection.
Analyse	Counting, loitering, queue/crowd, heat maps, license plates (ANPR). Pipeline: tracking.
Identify	Face recognition / biometric ID. HIGH-RISK biometric - a different build.

2 - Three places the AI can run (place every analytic)

```
On camera (edge) . in-camera detection, ships metadata + clips -> low bandwidth, private.
On a server ..... VMS + GPU, correlates one person across many cameras -> full-video bw.
In the cloud .... VSaaS subscription, scales -> but video leaves the premises (privacy + bw).
2026 default = HYBRID: detect on the camera, correlate and store on a server or the cloud.
```

3 - Watching events vs identifying people (EU AI Act + GDPR)

```
STANDARD .. event analytics (detect/count/intrusion): GDPR - lawful basis, signage, DPIA.
HIGH-RISK . biometric ID (face recognition/watchlist): EU AI Act Annex III(1) from 2 Aug 2026.
PROHIBITED real-time remote biometric ID in public spaces + emotion recognition: banned 2 Feb 2025.
```

4 - Add it: embed / assemble / build + the math

```
Embed via ONVIF Profile M + VMS . days-weeks; vendor models; you fit their feature set.
Assemble a CV stack ............ weeks-months; control analytics & data flow; you own tuning.
Build open models at the edge .. months; video never leaves device; no per-camera cloud fee.
Math: AI cuts false alarms ~90-95% (5,000->200 alerts/night for 50 cams); edge uplink KB vs ~200 Mbps cloud.
```

5 - Compliance gate - before launch (context, not legal advice)

- [ ] Establish a GDPR lawful basis for the cameras and post clear signage that filming is happening.
- [ ] Complete a Data Protection Impact Assessment (DPIA) for systematic monitoring of a public area.
- [ ] Set a retention period and delete on schedule; store event clips, not continuous footage, where possible.
- [ ] Encrypt footage in transit and at rest; limit access to people who genuinely need it.
- [ ] Keep biometric identification OFF by default; never run real-time remote ID in a public space (Article 5).
- [ ] For any biometric feature: EU AI Act high-risk obligations + human-in-the-loop verify; check NDAA camera rules.