Surveillance Privacy & Compliance Checklist - Pre-Deployment

Run these nine checkpoints before the system goes live. Engineering guidance, not legal advice - confirm specifics with qualified counsel.

Run it in order - the steps depend on each other

Purpose sets the lawful basis; the basis and the biometric answer set whether a DPIA is mandatory; the DPIA sizes the retention and the controls; the controls make the rights process possible. A system that can tick every box - AND show the document behind each tick - is one you can switch on and defend. The heaviest step is the biometric gate (step 5): if the system recognises people by their faces, several boxes get much harder.

1-3 DECIDE

- [ ] State each camera / zone's purpose in one sentence
- [ ] Pick a lawful basis; write the LIA if legitimate interests - GDPR Art. 6
- [ ] Run a DPIA before deploying if high-risk - GDPR Art. 35 / 36

4-6 BUILD

- [ ] Minimise: privacy zones, motion/event mode, audio off - Art. 5(1)(c) / 25
- [ ] Layered notice up before the cameras' coverage - Art. 13, EDPB 3/2019
- [ ] Clear the biometric gate before any recognition - Art. 9 / BIPA / AI Act

7-8 OPERATE

- [ ] Set a retention window; automate deletion across every tier - Art. 5(1)(e) / 17
- [ ] Least-privilege access, individual logins, tamper-resistant audit log - Art. 32
- [ ] Encrypt footage in transit and at rest; log every export - Art. 32

9 GOVERN

- [ ] Working subject-rights process; respond within one month - Art. 12(3)
- [ ] Record of Processing + a contract with every processor - Art. 28 / 30
- [ ] 72-hour breach plan ready; document cross-border; strictest region wins - Art. 33, Ch. V

The biometric gate - the step that changes everything (step 5)

Recording people and recognising them are different legal weights. The moment a system converts a face into a template and matches it, add a whole layer: an Art. 9 special-category condition (usually explicit consent) under GDPR; written informed consent, a public retention schedule, and private-right-of-action exposure ($1,000 / $5,000 per person) under Illinois BIPA (740 ILCS 14); and an EU AI Act Art. 5 check - some biometric uses are banned outright. Face recognition is the highest-liability feature in a surveillance system. Gate it hardest, or defer it.

This is engineering guidance, not legal advice. GDPR Reg. (EU) 2016/679 (Art. 5, 6, 9, 12-13, 17, 30, 32, 33, 35-36, Ch. V); EDPB Guidelines 3/2019 on video devices; Illinois BIPA 740 ILCS 14; EU AI Act Reg. (EU) 2024/1689 Art. 5; UK ICO CCTV guidance are summarised for planning - confirm specifics for your jurisdictions with qualified counsel.