City Surveillance Architecture & Governance Checklist

Plan a city or public-space surveillance build by its two defining loads — scale and privacy weight — before you buy hardware. Companion to the article; pair it with the surveillance cost model.

1 · The two loads - design for both at once

A city is defined by extreme scale (thousands of cameras, many vendors, many districts, many agencies) AND the heaviest privacy weight in surveillance, because it watches the public in spaces they cannot avoid. A design that answers only one of the two fails. Plan the architecture and the compliance posture together, from the first diagram.

2 · Federate - record local, stream on demand

Do not centralize. Build one system per district that records its own cameras locally, plus a thin layer that lets the centre search the whole city and open any camera on demand. Centralizing 5,000 cameras would need ~10 Gbps of constant backhaul and make the centre a single point of failure; federation carries only metadata and the views an operator opens. Hold a multi-vendor fleet together with ONVIF (Profile S/G/T/M) and specify performance against IEC 62676.

3 · Size storage and bandwidth (show the math)

Lever	Result
1 Mbps continuous	= 10.8 GB / camera / day
5,000 cams x 2 Mbps	= 108 TB / day
x 30-day retention	= 3.2 PB usable (~4.9 PB raw with RAID + headroom)
Backhaul: central vs federated	~10 Gbps constant vs ~200 Mbps on-demand

Retention length, recording mode, and storage tiering are the budget - not the camera spec.

4 · The biometric / legal gate - tick before any face matching

- [ ] Live face recognition of the public is OFF by default - a legal gate, not a toggle.
- [ ] EU AI Act Art. 5(1)(h): real-time remote biometric ID in public spaces is prohibited for law enforcement (in force 2 Feb 2025), bar narrow, court-authorised exceptions.
- [ ] A face template is GDPR Art. 9 special-category data; an ANPR / LPR plate is personal data, not biometric.
- [ ] Confirm the jurisdiction: the UK (Bridges judgment) and US city bans (e.g. San Francisco) differ sharply.
- [ ] Any biometric use: prior authorisation, a fundamental-rights / data-protection assessment, and a record.

5 · Privacy-by-design governance - build in, don't bolt on

- [ ] Documented lawful basis and purpose per camera and per analytic; cameras aimed no wider than needed.
- [ ] DPIA completed before go-live (GDPR Art. 35) - the default for large-scale public-space monitoring.
- [ ] Privacy masking over areas the system has no business watching (windows, interiors, a neighbour).
- [ ] Retention set to the minimum the purpose needs; scheduled, logged deletion (GDPR Art. 5(1)(e)).
- [ ] Role-based access per agency, with full audit logging of every view, search, and export.

Engineering guidance, not legal advice. The legal gate names the EU AI Act (Reg. (EU) 2024/1689) Art. 5, GDPR Art. 9 / Art. 35 / Art. 5(1)(e), EDPB Guidelines 3/2019, and the UK Bridges judgment; confirm specifics with qualified counsel before deploying any identification analytic.