Surveillance Retention & Lawful Deletion - Quick Reference

How long you may keep video, and how to delete it so it is provably gone. Engineering guidance, not legal advice - confirm specifics with qualified counsel.

Two limits, not one

Retention has a FLOOR (how long you MUST keep footage - sector minimums, legal hold, statute of limitations) and a CEILING (how long privacy law lets you keep it). The lawful window is the band between them. Pick a number inside it, write it down per camera group, and let the recorder enforce it automatically. The mistake that creates exposure is treating the floor as a target ('keep everything, just in case') - privacy law makes the short ceiling the default and makes you justify every extra day.

The retention & deletion rules (current to mid-2026)

Rule / source	What it governs	The limit	Duty
GDPR storage limitation - Art. 5(1)(e)	Ordinary footage of people	'No longer than necessary' - a few days; justify beyond ~72h	Erase when purpose ends
EDPB Guidelines 3/2019 (video)	Camera footage default	'Erased after a few days in most cases'	Short, documented window
GDPR right to erasure - Art. 17	One person's data on request	Respond within 1 month (Art. 12(3))	Reach every copy; 17(3) exceptions
BIPA - 740 ILCS 14/15(a)	Biometric templates (faces)	Purpose satisfied OR <= 3 yrs from last contact	Written public schedule + destroy
CCPA / CPRA - 1798.105 / .100	Personal info incl. video	Disclose period or criteria; honor delete	Notify third parties to delete
NIST SP 800-88	The act of deletion	Clear / Purge / Destroy	Overwrite, crypto-erase, or shred
Legal hold & sector minimums	Evidence - the floor	e.g. bank >= 45 days; preserve when litigation foreseeable	Hold the clip separately

PD = personal data. Named laws are the primary sources - confirm the article/section before relying on a row.

What 'delete' must actually reach

A routine delete only removes the file pointer - the bytes stay recoverable until overwritten. Real deletion uses overwrite (NIST Clear), block-erase or cryptographic erasure (Purge), or physical destruction (Destroy) - and it must reach EVERY copy: the primary recorder, nightly backups, DR replicas, exported clips on USB, and frames in alarm emails. A well-built VMS deletes routine footage for you via ring-buffer recording: new video overwrites the oldest once the window passes.

The right to erasure, in practice

Short retention means routine footage self-deletes fast, so an erasure request mainly bites DERIVED copies - analytics templates, saved case clips, watchlist entries. You have one month to respond (extendable to three for complex cases, with notice). You may refuse where the data is needed for a legal claim or legal obligation (Art. 17(3)) - a clip on legal hold is exactly that. Erasure is only feasible if you log where exports go.

The floor-and-ceiling check - run before you set a window

[ ] State each camera/zone's PURPOSE in one sentence (it defines what is 'necessary'). [ ] Find the FLOOR: sector minimums + a working legal-hold lane for incident clips. [ ] Find the CEILING: storage-limitation default (a few days to a few weeks) + any hard biometric cap. [ ] Pick a number INSIDE the band and document it per camera group. [ ] Make the recorder enforce it automatically (ring buffer / lifecycle rule). [ ] Ensure the delete date travels to EVERY tier - hot, warm, cold, archive - and to backups. [ ] Be able to erase one subject's derived data within one month.

This is engineering guidance, not legal advice. GDPR Reg. (EU) 2016/679 (Art. 5(1)(e), 12(3), 17); EDPB Guidelines 3/2019 on video devices; Illinois BIPA 740 ILCS 14/15(a); California CCPA/CPRA (Cal. Civ. Code 1798.105 / 1798.100, statute eff. 1 Jan 2026); NIST SP 800-88 Rev. 1; UK ICO CCTV guidance are summarised for planning - confirm specifics for your jurisdictions with qualified counsel.