Consent & Notice - Decision Guide

Notice and consent are two different jobs. Getting them right is an architecture decision, not paperwork. Engineering guidance, not legal advice - confirm specifics with qualified counsel.

The distinction that decides everything

NOTICE is telling people a camera runs - a one-way duty a good sign discharges, and one you almost always owe. CONSENT is getting each person's permission - a two-way, withdrawable choice with a high bar. A sign delivers notice; it is never, by itself, consent. Most ordinary cameras run on a non-consent basis plus notice. Consent becomes mandatory the moment you capture biometric data.

Notice or consent, by situation

Situation	What you need	Source	Sign enough?
EU - ordinary CCTV	Lawful basis (usually legitimate interest) + layered notice	GDPR Art. 6(1)(f); 12-13; EDPB 3/2019	Yes - if it meets para. 114-116
EU - facial recognition	Explicit consent (Art. 9(2)(a)) or another Art. 9 exception	GDPR Art. 9; 4(14)	No - a sign is not explicit consent
US - ordinary video	Notice; CCPA notice at collection where it applies	CCPA/CPRA 1798.100	Usually - with proper notice
US - audio with video	All-party consent in ~12 states	18 U.S.C. 2511; state wiretap laws	No - silence is not consent
US (Illinois) - biometrics	Informed written release BEFORE capture + public policy	BIPA 740 ILCS 14, 15(b)/15(a)	No - you need a signed release

Valid consent (Art. 4(11) + Art. 7) - when you do need it

Four ingredients: (1) freely given - a real no-penalty choice; (2) specific - one defined purpose; (3) informed - knows who, what, why; (4) unambiguous - a clear affirmative act. Plus Art. 7: you can prove it, you present it separately in plain language, and withdrawal is as easy as giving it. NOT valid: a pre-ticked box, bundling several purposes into one tick, or consent under a power imbalance (employer over employee).

The first-layer sign checklist (EDPB 3/2019 paras 114-116)

A compliant warning sign carries: the PURPOSE of the surveillance; the CONTROLLER's identity and contact; the existence of the data subject's RIGHTS; the RETENTION period; any SURPRISING detail (e.g. footage shared with third parties); and a POINTER to the full notice (QR / reception / web). Position it at a reasonable distance so a person recognises the situation BEFORE entering the monitored area. 'CCTV in operation' alone is decorative, not notice.

Biometrics & the workplace - consent, not a sign

A face/iris/voice template needs EU explicit consent (Art. 9(2)(a)) or, in Illinois, a signed BIPA 15(b) release BEFORE capture plus a public retention policy (15(a)) - neither of which a wall sign delivers, and an open-area camera cannot obtain from passers-by. At work, ordinary cameras run on legitimate interest + notice (employee consent is rarely free - power imbalance); but a biometric time clock in Illinois still needs the written release. US audio: disable the microphone unless you have all-party consent where required.

Run before you procure

[ ] Decide the lawful basis BEFORE the camera records (usually legitimate interest, not consent). [ ] First-layer sign meets the para. 114-116 content + positioning test; full notice reachable. [ ] Biometric analytics OFF by default; enabling it is a documented decision with its own consent flow. [ ] Where you cannot get consent from everyone in frame, do NOT build the template. [ ] Illinois biometrics: signed 15(b) release + public 15(a) policy in place; geo-fence capture. [ ] Audio off unless all-party consent is obtained where the state requires it.

This is engineering guidance, not legal advice. GDPR Art. 4(11)/4(14)/6/7/9/12-13 and Recitals 32/42/43, EDPB Guidelines 3/2019, Illinois BIPA 740 ILCS 14, CCPA/CPRA (Cal. Civ. Code 1798.100), the EU AI Act Art. 5, and 18 U.S.C. 2511 are summarised for planning - confirm the specifics for your jurisdictions with qualified counsel.