Privacy-Preserving Surveillance - Technique & Compliance Guide

Masking, redaction, and de-identified analytics let a system keep its security value and shed most of its privacy risk. Engineering guidance, not legal advice - confirm specifics with qualified counsel.

The distinction that decides everything: can it be undone?

If the original un-obscured image still exists or the obscuring can be computed back, you have PSEUDONYMISED the data (GDPR Art. 4(5)) - it is still personal data and every GDPR duty applies (Recital 26). If the original is genuinely destroyed with no key or recoverable copy, you may have ANONYMISED it - which leaves GDPR scope (Recital 26), but only if re-identification is not possible by any means reasonably likely to be used. The question is never 'did we blur it?' - it is 'can the identity be recovered?'

The four operations, side by side

Technique	Where applied	Reversible?	GDPR status
Privacy mask (ONVIF)	On the camera, fixed zone	No - never recorded	Outside scope for that zone
Dynamic masking, reversible	VMS live view, original kept	Yes - by design, with key	Pseudonymisation - still personal
Permanent masking	Burned into the recording	Only if pixels destroyed	Anonymisation IF irreversible
Redaction	At export of stored footage	Must be irreversible on copy	Anonymous copy if unrecoverable
De-identified analytics	Edge / processing layer	No - identity never kept	Outside scope if no re-id

De-identification has a vocabulary (Art. 29 WP 05/2014; ISO/IEC 20889; NISTIR 8053)

Two families: RANDOMISATION (noise addition, permutation, differential privacy) alters the data to break the link; GENERALISATION (aggregation, k-anonymity, l-diversity, t-closeness) dilutes detail so records merge. Pseudonymisation is NOT anonymisation. Test every method against three residual risks - singling out an individual, linking records across datasets, and inferring new facts. A method that leaves any of the three open has not anonymised the data.

The blur trap - pixelation and blur are usually reversible

Blur and pixelation scramble identifying information; they do not remove it. In 'Defeating Image Obfuscation with Deep Learning' (2016), neural networks re-identified pixelated faces (16x16) about 57% of the time (72% in the top five) across 530 individuals, and blurred faces over 50% of the time on a 40-face set; newer work reconstructs recognisable faces. So a light blur is pseudonymisation, not anonymisation. To make an export genuinely anonymous, destroy the pixels (solid fill or replacement), not smudge them.

The strongest control: edge metadata-only analytics

Run the analytic on the camera or edge box and send only the result - a count, a dwell time, an event - so the central system holds numbers, not faces. A camera streaming H.265 at 4 Mbps uploads ~43.2 GB/day of identifying video; emitting one ~200-byte count record every 5 minutes is ~57.6 KB/day - roughly a 750,000x reduction, with the identifying content dropping to zero. Nothing recognisable leaves the device, so there is no biometric data to protect and far less to retain.

Run before you deploy

[ ] Specify each privacy control by its effect on recoverability, not how strong the blur looks. [ ] If you mask the live view, govern the stored original as the personal data it remains (basis, retention, DSAR). [ ] For an 'anonymous' export, destroy the pixels - do not ship a recoverable blur. [ ] Prefer edge metadata-only analytics where a count or event is enough; disable facial recognition and audio you do not need. [ ] For formal de-identification, document the technique and test singling out / linkability / inference. [ ] Treat reversible masking (key/dual-authorisation unmask) as pseudonymisation - keep GDPR controls on it.

This is engineering guidance, not legal advice. GDPR Recital 26, Art. 4(5), Art. 4(14)/9, Art. 25; EDPB Guidelines 3/2019; Article 29 WP Opinion 05/2014; ISO/IEC 20889:2018; NISTIR 8053; ONVIF Media2 privacy masks; and the 2016 'Defeating Image Obfuscation' benchmark are summarised for planning - confirm the specifics for your jurisdictions and products with qualified counsel.