

GDPR для видеонаблюдения - стартовый комплаенс

Камера, снимающая людей, обрабатывает персональные данные. Задайте рамку до закупки. Инженерное руководство, не юр. совет - уточняйте конкретику у юриста.

Сначала - правовое основание (GDPR ст. 6)

Для большинства частных операторов это законный интерес (ст. 6(1)(f)) - ЗАДОКУМЕНТИРОВАННЫЙ тест из трёх частей, а не ярлык: (1) Цель - реальный, текущий, чётко сформулированный интерес (не гипотетический); (2) Необходимость - нет менее инвазивного способа, только нужные для цели данные; (3) Баланс - ваш интерес не перевешивает права и разумные ожидания людей (спортзал, туалет, ресторан - против вас). Органы власти -> публичная задача (6(1)(e)); запись по закону -> правовая обязанность (6(1)(c)); согласие (6(1)(a)) редко работает для открытого CCTV.

Обязанности GDPR, каждая привязана к статье

Обязанность	Что это значит для системы	Основа
Правовое основание	Зафиксируйте до записи; LIA для законного интереса	ст. 6
Минимизация данных	Только нужные данные; без аудио, если не требуется	ст. 5(1)(c)
Лимит хранения	Держите несколько дней; удаляйте автоматически	ст. 5(1)(e)
Права субъектов	Доступ (+ маскировка других) и удаление; ответ за 1 мес.	ст. 15/17
Безопасность	Шифрование при передаче/хранении + контроль доступа	ст. 32
Процессор и трансфер	Письменный DPA с облачной VMS; механизм при вывозе из ЕЭЗ	ст. 28 / гл. V
DPIA и реестр	DPIA до запуска при масштабе/биометрии; ведите реестр	ст. 35 / 30

Биометрические ворота (GDPR ст. 9)

Запись видео идёт по ст. 6. РАСПОЗНАВАНИЕ ЛИЦ превращает лицо в биометрический шаблон (ст. 4(14)) = особая категория (ст. 9), ЗАПРЕЩЕНО по умолчанию, если нет исключения по ст. 9(2). Для коммерческого наблюдения единственное реальное исключение - явное согласие, и нужно оно от ВСЕХ в кадре, а не только от внесённых в базу. В открытых местах это обычно невозможно, поэтому публичное распознавание лиц по GDPR почти всегда незаконно. Считайте биометрию осознанным решением с согласием, DPIA и визой юриста.

Сообщите людям: двухслойное уведомление (ст. 12-13)

Первый слой (знак на уровне глаз до зоны): цель наблюдения, личность и контакт оператора, что есть права, и где найти больше. Второй слой (полное уведомление по ст. 13 на ресепшен, сайте или по QR-коду): правовое основание и интерес, срок хранения, кому передаётся видео, выходит ли из ЕС, и как осуществить права. Одной надписи «ведётся видеонаблюдение» недостаточно.

Пройдите до закупки

[] Цель записана для каждой камеры (конкретно, не «общая безопасность»). [] Основание выбрано + LIA задокументирован. [] Распознавание лиц ВЫКЛ, если нет согласия + DPIA + юриста. [] Двухслойные знаки подготовлены. [] Хранение - дни, удаление автоматическое. [] Система умеет искать, выгружать и маскировать для запросов доступа. [] DPA подписан с облаком/процессором; механизм трансфера при вывозе из ЕЭЗ. [] DPIA до запуска; ведётся реестр обработки.

Это инженерное руководство, не юридический совет. Тест основания, ворота ст. 9, нормы знаков и хранения и цифры штрафов даны для планирования - уточняйте конкретику вашей юрисдикции у квалифицированного юриста. Штрафы GDPR - до EUR 20 млн или 4% мирового оборота (ст. 83). EU AI Act добавляет слой над GDPR, его даты меняются (перепроверяйте).