

Приватное видеонаблюдение - руководство по технике и комплаенсу

Маскирование, редактирование и обезличенная аналитика сохраняют пользу для безопасности и снимают почти весь риск приватности. Инженерное руководство, не юр. совет - уточняйте конкретику у юриста.

Различие, которое решает всё: можно ли это отменить?

Если оригинал без маски всё ещё существует или скрытие можно вычислить обратно - вы ПСЕВДОНИМИЗИРОВАЛИ данные (GDPR ст. 4(5)): это персональные данные, и все обязанности GDPR действуют (Рек. 26). Если оригинал по-настоящему уничтожен, без ключа и копии - возможно, вы АНОНИМИЗИРОВАЛИ их, и тогда они вне GDPR (Рек. 26), но лишь если реидентификация невозможна любыми средствами, разумно вероятными к применению. Вопрос не «размыли ли мы?», а «можно ли восстановить личность?».

Четыре операции рядом

Техника	Где применяется	Обратимо?	Статус по GDPR
Privacy-маска (ONVIF)	На камере, фикс. зона	Нет - не пишется	Вне сферы для этой зоны
Динам. маска, обратимая	Просмотр VMS, оригинал хранится	Да - по замыслу, с ключом	Псевдонимизация - персон. данные
Постоянная маска	Вшита в запись	Только если пиксели уничтожены	Анонимизация, ЕСЛИ необратимо
Редактирование	При экспорте записи	Должно быть необратимо на копии	Анон. копия, если невозможна
Обезличенная аналитика	Edge / слой обработки	Нет - личность не хранится	Вне сферы, если нет реид.

У обезличивания есть словарь (Art. 29 WP 05/2014; ISO/IEC 20889; NISTIR 8053)

Два семейства: РАНДОМИЗАЦИЯ (добавление шума, перестановка, differential privacy) меняет данные, разрывая связь; ОБОБЩЕНИЕ (агрегация, k-anonymity, l-diversity, t-closeness) огрубляет детали, сливая записи. Псевдонимизация - НЕ анонимизация. Проверьте каждый метод на три риска: выделение человека, связывание записей между наборами и вывод новых фактов. Метод, оставляющий открытым хоть один из трёх, данные не анонимизировал.

Ловушка блюра - пикселизация и размытие обычно обратимы

Блур и пикселизация перемешивают идентифицирующую информацию, но не удаляют её. В работе 'Defeating Image Obfuscation with Deep Learning' (2016) сети опознали пикселизованные лица (16x16) примерно в 57% случаев (72% в топ-5) на 530 людях и размытые лица свыше 50% на наборе из 40 лиц; новые работы восстанавливают узнаваемые лица. Значит, лёгкий блур - это псевдонимизация, не анонимизация. Чтобы экспорт был по-настоящему анонимным, уничтожьте пиксели (заливка или замена), а не размазывайте их.

Сильнейший контроль: аналитика только метаданных на краю

Считайте аналитику на камере или edge и шлите только результат - счётчик, время пребывания, событие - чтобы центр хранил числа, а не лица. Камера H.265 на 4 Мбит/с грузит ~43,2 ГБ/день идентифицирующего видео; одна запись ~200 байт каждые 5 минут - это ~57,6 КБ/день, примерно в 750 000 раз меньше, а идентифицирующее содержимое падает до нуля. Узнаваемое не покидает устройство: нет биометрии для защиты и куда меньше для хранения.

Пройдите до развёртывания

[] Задавайте каждый контроль по влиянию на восстановимость, а не по силе блюра на вид. [] Маскируете просмотр - управляйте хранимым оригиналом как персональными данными (основание, хранение, запросы). [] Для «анонимного» экспорта уничтожайте пиксели - не отдавайте восстановимый блур. [] Предпочитайте аналитику только метаданных на краю, где хватает счётчика; отключите ненужные распознавание лиц и аудио. [] Для формального обезличивания задокументируйте метод и проверьте выделение / связывание / вывод. [] Обратимую маску (снятие ключом / двойной авторизацией) считайте псевдонимизацией - оставьте на ней контроли GDPR.

Это инженерное руководство, не юридический совет. GDPR Рек. 26, ст. 4(5), 4(14)/9, 25; EDPB Guidelines 3/2019; Article 29 WP Opinion 05/2014; ISO/IEC 20889:2018; NISTIR 8053; ONVIF Media2 privacy masks; и бенчмарк 'Defeating Image Obfuscation' (2016) даны для планирования - уточняйте конкретику ваших юрисдикций и продуктов у юриста.