

MEDIA, 3D RENDER AND THE GPU — WHERE EACH STEP RUNS, AND WHAT PROTECTS IT

left is closest to the person, right is closest to the GPU; the further right a step runs, the further the media has to travel

Heavy box = the media never leaves the device. Red dashed = a common mistake.

	closer to the person				closer to the GPU
	DEVICE	EDGE	SYSTEM OF RECORD	KUBERNETES CLUSTER	HOSTED GPU OR API
Images	<div>Client preview canvas or WebGPU resize before upload</div>	<div>Transform on request Cloudflare Images: resize, format, crop; cached</div>	<div>Private original R2 or S3, never public; Xano holds record and key</div>	<div>Batch in C libvips or ImageMagick pods; policy.xml limits coders</div>	<div>Adobe Firefly Services Photoshop, Lightroom APIs; the file goes to Adobe</div>
3D game render	<div>Real-time render WebGPU or native on the player's GPU; WGSL, SPIR-V</div>	<div>Asset delivery glTF and KTX2 from cache; signed URLs, no edge GPU</div>	<div>Asset catalog versions, licences, owners; the record decides access</div>	<div>Build and bake texture compression, lightmaps; GPU Operator for GPU pods</div>	<div>Offline or streamed render farms, pixel streaming on CoreWeave- or OCI-class</div>
AI media	<div>On-device model small upscale or segment; media stays on the device</div>	<div>Workers AI classify, caption, moderate with Cloudflare's models</div>	<div>Consent and rights is this face, voice or asset cleared for this use?</div>	<div>Self-hosted models GPU node pools; the data stays in your account</div>	<div>Generative APIs Firefly, hosted image models; read retention terms</div>

PROTECTION RULES · EVERY COLUMN

<div>base64 is not protection it is an encoding: about a third larger, and it hides nothing</div>	<div>Kubernetes Secrets are base64 turn on encryption at rest or an external KMS; tighten RBAC</div>	<div>Lock down ImageMagick policy.xml: disable unused coders; cap memory, time and image size</div>	<div>Strip before egress remove EXIF GPS and device IDs; signed, expiring URLs only</div>
--	---	--	--