Gate records and the Data Protection Act, 2020

A gate log is personal data: names, ID details, vehicle plates, photographs, and the times people come and go. This page sets out how GateLog is built to help your organization meet Jamaica's eight data-protection standards — and why the paper book cannot.

YOUR ORGANIZATION — DATA CONTROLLER

You decide what is collected at your gates and why, and you register with the Office of the Information Commissioner (OIC) as required.

GATELOG (STACKCURIOUS LLC) — DATA PROCESSOR

We process gate records only on your instructions, under contract, and never use or share your data for any other purpose.

WHAT THE GATE COLLECTS — AND NOTHING MORE

Only what a security post needs: **who** (name, company, host), **proof** (photo, ID where your policy requires it), **what** (vehicle plate, purpose), and **when** (time in / time out). No browsing history, no location tracking, no biometric matching.

THE EIGHT STANDARDS — HOW GATELOG DELIVERS EACH ONE

DPA STANDARD	HOW GATELOG MEETS IT
1 · Fair & lawful processing	Collection happens openly at a manned gate for a legitimate security purpose; on-screen and signage wording is configurable so visitors are informed at the point of capture.
2 · Purpose limitation	Records exist for premises security and safety, and are used for nothing else. GateLog never sells, mines, or repurposes gate data.
3 · Adequate, relevant, not excessive	Capture fields are configured per gate — each gate collects only the fields your policy defines, nothing speculative.
4 · Accuracy	Entries are time-stamped at capture with photo evidence. Corrections don't overwrite: they're logged with who changed what, when, and why.
5 · Retention	Photos and media cycle out automatically on your retention policy (incident media: 12 months); retention periods are disclosed in-product. The paper book keeps everything forever, in a box.
6 · Data-subject rights	Any person's records can be found in seconds — so a subject-access request is an export, not an archaeology project. Deletion requests are actionable and auditable.
7 · Security safeguards	Encrypted in transit and at rest; role-based access (a guard, a manager, and head office each see only their scope); multi-factor authentication for administrators; every access path logged; point-in-time backups.
8 · Cross-border transfer	Data is hosted in hardened, certified cloud data centres (AWS, US East) under contractual safeguards with encryption throughout — a documented transfer arrangement your DPO can stand behind, versus a photocopied page leaving the building unrecorded.

The paper book, measured against the same standards: unencrypted, uncontrolled access, no retention policy, no correction trail, unsearchable for subject-access requests, and routinely stored off-site with no record of who has read it. Under the DPA, the book is not a record-keeping system — it is a liability.

PRACTICAL NOTES FOR YOUR DPO

Breach response
Access is logged and scoped, so "what was exposed, about whom" is answerable within the 72-hour notification window.

Processing agreement
A signed controller–processor agreement is part of onboarding, covering instructions, confidentiality, sub-processors and deletion on exit.

Your data, always
Full export available at any time; on contract end, your records are returned and purged on a documented schedule.

OIC registration
Controller registration remains your obligation — GateLog's documentation (this page, retention config, audit trail) supports your filing.