

Privacy & Consent Notice

A drafting template for facilities operating an intelligent monitoring system in Nigeria, oriented to the Nigeria Data Protection Act 2023.

This is a template, and it is not legal advice. It is a starting point drafted to save your lawyer time, not to replace them. Every deployment differs in purpose, lawful basis and retention, and a notice that does not match what your system actually does is worse than no template at all. **Have this reviewed and adapted by a qualified Nigerian legal practitioner before you publish or display it.** Wise Hustlers Technologies accepts no liability for use of this template as-is.

How to use it. Everything shown as [\[LIKE THIS\]](#) is a blank you must fill in. Everything shown as an instruction in italics is guidance for the drafter and should be deleted before the notice is issued. Delete any section that does not describe your deployment — an inaccurate notice creates exposure rather than reducing it.

Part A — Who is responsible

Field	Your entry
Data controller The organisation that decides why the monitoring exists	<u>[FULL REGISTERED NAME OF YOUR ORGANISATION]</u>
Registered address	<u>[ADDRESS]</u>
Premises covered by this notice	<u>[SITE NAME AND ADDRESS]</u>
Contact for privacy matters	<u>[NAME / ROLE]</u> , <u>[EMAIL]</u> , <u>[PHONE]</u>
Data Protection Officer Where your organisation is required to appoint one, or has chosen to	<u>[NAME AND CONTACT, OR "Not appointed — see contact above"]</u>
Data processor The party operating the system on your instructions	Wise Hustlers Technologies Private Limited, acting solely on the controller's documented instructions
Notice version and date	Version <u>[1.0]</u> , effective <u>[DATE]</u>

Part B — What we monitor and why

Drafting note: state the real purpose, specifically. "Security" on its own is not a purpose a regulator will accept. Delete the examples that do not apply.

[ORGANISATION NAME] operates an intelligent monitoring system at the premises named above. We use it for the following purposes, and for no other purpose:

- [e.g. Protecting the safety of people on the premises]
- [e.g. Preventing and investigating theft, damage and unauthorised access]
- [e.g. Controlling access to restricted areas]

- [e.g. Measuring crowd density at peak times so we can manage capacity safely]

State what you will not do with it. A notice is far more credible when it names the excluded uses. For example: *“We do not use this system to monitor individual staff productivity, and we do not use it to make automated decisions about any individual.”* Only include such a statement if it is true and you will hold to it.

Part C — What the system actually processes

Drafting note: tick the rows that match your configuration and delete the rest. Your installer will confirm which apply.

Category	In use?	What this means
Live images	<u>[YES/NO]</u>	Images viewed in real time by authorised staff, not retained.
Recorded video	<u>[YES/NO]</u>	Footage retained for a fixed period, then deleted automatically.
Event records	<u>[YES/NO]</u>	A record that something occurred, on which camera, at what time — without a stored image.
Facial recognition / biometric matching	<u>[YES/NO]</u>	A numeric template derived from a face, compared against a list this organisation maintains. This is sensitive personal data and requires its own lawful basis.
Vehicle plate capture	<u>[YES/NO]</u>	Plate details recorded on entry or exit. Personal data where it identifies an individual.
Anonymous counting only	<u>[YES/NO]</u>	Numbers of people, with no identification of anyone.

If you answered YES to biometric matching, do not skip this. Biometric data used to identify a person is treated as sensitive personal data. It needs a lawful basis that specifically supports processing sensitive data, a documented necessity and proportionality assessment, and — in most private-premises deployments — a genuine, freely given and withdrawable consent, or a clearly evidenced alternative basis. If you cannot articulate that basis in a sentence, the honest conclusion is usually that this feature should be switched off. It can be.

Part D — Our lawful basis

Drafting note: name the basis you actually rely on and state why it applies. Do not list several as a hedge — a regulator reads that as not having decided.

Before you choose anything other than consent for biometrics, read this.

Section 30(1) of the Act does offer several alternative grounds for processing sensitive personal data. But the NDPC's General Application and Implementation Directive 2025 states at Article 18(1)(b) that **consent is required for the processing of sensitive personal data**, and Article 17(5) adds that reliance on an unsupported alternative basis “shall be strictly scrutinised during NDP Act compliance audits.” Where the Act and the Directive conflict the Act prevails (GAID Art 3(2)) — so consent is not strictly the only lawful route. It is, however, the route the regulator expects, and departing from it is a decision to take with legal advice and to document.

Processing activity	Lawful basis relied on and why
<u>[e.g. General premises monitoring]</u>	<u>[STATE THE BASIS AND THE REASON IT APPLIES]</u>
<u>[e.g. Biometric matching at the staff entrance]</u>	<u>[STATE THE BASIS. If consent, explain how it is freely given and how it can be withdrawn without detriment.]</u>

Part E — Where your data is held

Drafting note: delete the two options that do not apply to your deployment.

- **On our premises.** All processing and storage take place on equipment located at [SITE]. Recorded material does not leave the premises.
- **Hosted in Nigeria.** Data is held in a hosting facility located in Nigeria at [FACILITY / PROVIDER].
- **Hosted outside Nigeria.** Data is held in [COUNTRY / REGION]. *If you select this, you must state the transfer mechanism you rely on and complete Part F.*

Part F — International transfers

Delete this entire section if no data leaves Nigeria.

Where personal data is transferred outside Nigeria, we do so on the basis of [STATE THE TRANSFER MECHANISM RELIED ON], and we apply the following safeguards: [LIST SAFEGUARDS — e.g. contractual clauses, encryption in transit and at rest, restrictions on onward transfer]. You may request further information about these arrangements using the contact details in Part A.

Part G — How long we keep it

Category	Retention period
Recorded video	<u>[e.g. 30 days]</u> , after which it is deleted automatically
Event records	<u>[e.g. 30 days]</u> , after which they are deleted automatically
Biometric templates <i>(if used)</i>	For as long as the individual remains on our list, and deleted on removal
Material subject to an active investigation	Until the investigation concludes, then deleted
Access and audit logs	<u>[e.g. 12 months]</u>

Deletion is performed automatically by the system on expiry of the period above. It does not depend on a member of staff remembering to act.

Part H — Who can see it

- Named, authorised members of our own staff, each with an individual login, whose access to this material is recorded in an audit log. We do not use shared accounts.
- Wise Hustlers Technologies, as our processor, strictly to operate and support the system on our documented instructions.
- Law enforcement or a regulator, where we are lawfully required or permitted to disclose.
- [ANY OTHER RECIPIENT — e.g. insurer, appointed security contractor. Name them, or delete this line.]

We do not sell this data, and we do not share it for anyone's marketing or commercial purposes. Every viewing, search and export is logged against a named person with the reason they gave.

Part I — Your rights

As an individual whose personal data we process, you have the following rights under the Nigeria Data Protection Act 2023 (sections 34 to 37):

- **To be told what we hold and why** — without constraint or unreasonable delay: the purposes of processing, the categories of data, who receives it (particularly any recipients in other countries), how long we keep it, where we got it if not from you, and whether any decision about you is made by automated means.
- **To get a copy** of your personal data in a commonly used electronic format. Note that the Act permits a controller to ask you to bear some or all of the cost where providing it would be unreasonably costly — [state your own position on charging, or delete this sentence].
- **To have it corrected**, or deleted where correction is not feasible.
- **To have it erased** without undue delay. We must also erase it on our own initiative once it is no longer necessary, or once we have no lawful basis to keep it.
- **To restrict processing** while a dispute, an objection or a legal claim is resolved.
- **To object** to processing. We must stop unless we can demonstrate overriding public interest or legitimate grounds. **For direct marketing your right to object is absolute** — we must stop, with no balancing exercise.
- **To withdraw consent** at any time, where we rely on consent. The Act requires that withdrawing be as easy as giving it. Withdrawal is not retroactive.
- **Not to be subject to a decision based solely on automated processing**, including profiling, that produces legal or similarly significant effects — and, where such processing is permitted, to obtain human intervention, to express your view, and to contest the decision.
- **To complain to the Nigeria Data Protection Commission**, and to bring a separate civil claim for damages.

Drafting note — data portability. Do not list portability as a free-standing right. Section 38(1) of the Act is *enabling*: it provides that the Commission *may* make regulations establishing a right of data portability. Until it does, claiming to grant it here overstates the position. Have your legal adviser confirm the current position before publishing.

To exercise a right, contact **[CONTACT NAME / ROLE]** at **[EMAIL]**. We will respond within **[STATE THE PERIOD YOU COMMIT TO]**. There is no charge for making a request.

If you are not satisfied with our response, you may complain to the Nigeria Data Protection Commission.

A practical limit worth stating honestly. If you ask for a copy of footage that also shows other people, we may need to obscure them before releasing it, because their privacy rights are engaged too. Saying so in the notice avoids an argument later.

Part J — Withdrawing consent

Include this section only where you actually rely on consent.

Where we rely on your consent, you may withdraw it at any time by contacting **[CONTACT]**. Withdrawal is as easy as giving consent, it takes effect going forward, and it will not disadvantage you. **[Where an alternative arrangement exists — e.g. a card or a manual sign-in instead of biometric entry — describe it here. If no alternative exists, consider carefully whether the consent can be said to be freely given at all.]**

Part J2 — Your impact assessment obligation

For cameras in a place the public can reach, a Data Protection Impact Assessment is mandatory — not advisable. GAID Article 28(3) lists, among the processing types that require one: systematic monitoring; processing involving sensitive personal data; “deployment of surveillance cameras in places that may be accessed by members of the public”; educational services involving pupil records; and hospitality services. Most deployments covered by this notice hit at least two of those.

- The assessment must be carried out **before** the processing starts (NDPA s.28(1)).
- It **must be vetted by a DPO accredited by the Commission** (GAID Art 28(4)). A vendor’s draft is an input to that, not a substitute for it.

- It is **filed with the Commission**, and its outcome forms part of your Compliance Audit Return (GAID Art 28(5)).
- Failing to carry one out may result in a restriction on the platforms through which you contact data subjects at all (GAID Art 28(6)).
- If residual high risk remains after mitigation, you must consult the Commission (NDPA s.28(2)).

Part K — Entrance signage

A notice this long cannot be read at a doorway. Display the short version below at every entrance to the monitored area, in a size readable from a normal approach distance, and place the full notice where the sign points.

THIS AREA IS MONITORED

[ORGANISATION NAME] operates a monitoring system here for **[PURPOSE — e.g. the safety and security of people and property]** .

[INCLUDE ONLY IF TRUE: This system uses facial recognition.]

Recordings are kept for **[PERIOD]** and then deleted. For the full privacy notice, or to exercise your rights over your data, contact **[EMAIL / PHONE]** or see **[WEB ADDRESS]** .

If the system uses facial recognition, the sign must say so. Discovering it later is the single fastest route to a complaint, and it turns a lawful deployment into a trust problem you cannot argue your way out of.

Part L — Consent record

Use this only where you rely on consent — for example a staff or member biometric enrolment. A tick box with no record is not evidence of consent.

Field	Record
Name of individual	<u>[NAME]</u>
What they consented to	<u>[SPECIFIC PROCESSING — e.g. enrolment of a facial template for staff entrance access]</u>
Notice version shown	<u>[VERSION AND DATE]</u>
Date and method of consent	<u>[DATE, AND HOW IT WAS GIVEN]</u>
Alternative offered	<u>[WHAT THEY COULD HAVE CHOSEN INSTEAD]</u>
Withdrawn on	<u>[DATE, IF APPLICABLE]</u>

Part M — Sector-specific reminders

Setting	Additional consideration
Schools	Processing involves children, and GAID Art 18(1)(d) requires consent for processing a child's personal data. Education is a listed sector for registration, so schools get no exemption. Parental consent, a strict retention ceiling, and no processing beyond the stated safeguarding purpose should be treated as mandatory.
Hospitals	Health context makes almost everything sensitive. Exclude clinical areas by default and review the deployment with the facility's own privacy lead.
Hotels	Public circulation areas only. Never in rooms, in corridors serving rooms, or in any area of expected privacy.
Workplaces	Employment law applies alongside data protection. Notify workers, consult where required, and record a proportionality assessment.
Churches	Heightened sensitivity around attendance at a place of worship. Signage at every entrance and a named contact for the congregation. Note carefully: the NDPC exempts faith-based organisations from the requirement to <i>register</i> as a controller of major importance. That exemption is from registration <i>only</i> — lawful basis, consent, security, breach notification, impact assessments and data subject rights all continue to apply in full.
Public spaces	The highest-scrutiny category. Public consultation and a published impact assessment should precede deployment.

Template issued by Wise Hustlers Technologies · info@wise-hustlers.com · wise-hustlers.com/your-data-is-protected

Provided as a drafting aid only. It is not legal advice and must be reviewed by a qualified Nigerian legal practitioner before use.