



DATA PRIVACY | REGULATORY

Invisible data collection through a privacy lens

17 September 2026 7 min read

by Ahmore Burger-Smidt, Director and Head of Regulatory

More than seven million pairs of Meta's Ray-Ban smart glasses were sold worldwide in 2025. That figure alone should make any compliance officer focus. Apple's AirPods Pro 3, launched in September 2025, now monitor heart rate and translate live conversations using artificial intelligence.^[1] A next-generation Apple AirPods with an embedded camera is in advanced testing. These are not consumer curiosities, they are data collection instruments that walk through office doors, and POPIA has something to say about every byte they capture.

The global regulatory response has been swift. France's CNIL warned in May 2026 that smart glasses risk normalising surveillance that is "*almost invisible and omnipresent*."^[2] Germany's Hamburg data protection commissioner concluded that covert filming with these devices violates data protection law, and a sales ban is under active review.^[3] The UK's ICO has formally written to Meta demanding compliance information,^[4] and a US class action alleges the glasses are a "surveillance nightmare disguised as fashion."^[5] In East Africa, a Russian vlogger was identified in early 2026 recording intimate encounters with women in Kenya and Ghana using Meta smart glasses and posting the footage online for profit.^[6]

South Africa is not insulated from any of this. POPIA's framework for special personal information, its transparency obligations, and its transborder transfer restrictions are all directly engaged.

The POPIA Exposure: Five Critical Risk Areas

Biometric and Health Data as Special Personal Information

Biometric information occupies a privileged category under POPIA. It is classified as "special personal information," and processing it is generally prohibited unless a specific statutory exception applies, most commonly, explicit consent or a substantial public interest justification. The practical implications are significant. Meta's smart glasses capture facial features, voiceprints, and video footage of identifiable individuals. Apple's AirPods Pro 3 collect heart rate, motion, and calorie data via an in-ear optical sensor, transmitting this to Apple's Health ecosystem and, with user permission, to third-party fitness applications.^[7]

Bystander and Third-Party Rights

Every data subject has the right to know when personal information about them is being collected. That right is effectively annihilated by a device designed to record people covertly. Smart glasses are, by their nature, silent observers. The sole notification mechanism on Meta's Ray-Ban glasses is a small LED light, which a peer-reviewed CHI 2026 study concluded is "inadequate" as a bystander safeguard.^[8] Regulators across France, Germany, and the Netherlands have reached the same conclusion. The legal difficulty is plain: section 11 of POPIA requires a responsible party to demonstrate a lawful basis for processing which becomes a near-impossibility when the data subject has no knowledge that processing is occurring at all.

Transparency and Notice Failures

Section 18 of POPIA requires reasonably practicable steps to ensure data subjects know what information is being collected, why it is being collected, and who is responsible. What the major technology companies have been doing sits uncomfortably with that obligation. Meta's April 2025 privacy policy update removed the option for users to disable voice recording storage and enabled AI features by default.^[9] A Swedish investigation in early 2026 revealed that intimate footage, including nudity and financial information, was reviewed by human contractors in Kenya without adequate disclosure to users.^[10] That kind of murkiness can be said to be fundamentally inconsistent with POPIA's transparency mandate.

Transborder Data Transfers

Personal information may only leave South Africa where the recipient country provides an adequate level of protection, or where binding corporate rules or consent apply. This is not an abstract concern. Meta's routing of footage captured by South African users to contractor facilities in Nairobi for AI training annotation raises serious questions about compliance with section 72.^[11] Apple's transmission of aggregated health and activity data to its US-based servers engages the same provision.

Security of Processing

Responsible parties must secure the integrity and confidentiality of personal information through appropriate technical and organisational measures. Section 19 demands nothing less. The revelation that Meta's AI training pipeline could not distinguish between mundane footage and deeply sensitive content, and that no adequate filtering existed, represents a failure that would be difficult to defend under any reasonable reading of the provision.

What Does This Mean for Organisations

The Information Regulator's 2025/26 Annual Performance Plan signals a firmer enforcement posture,^[12] including a new compliance monitoring programme, a Code of Conduct for data collection at controlled entry points (covering biometric systems and surveillance technologies at business premises), and mandatory e-portal breach reporting since April 2025. Against this backdrop, South African organisations should consider, amongst others, the following:

- Consider whether to restrict smart glasses and AI-enabled earbuds in offices, boardrooms, client-facing areas, and controlled environments. Also, review workplace policies on wearable devices.
- Update privacy notices to address the possibility that employees, visitors, or clients may be recorded by wearable devices, and specify the organisation's position on such recording.
- Conduct Personal Information Impact Assessments (PIIAs) as required by Regulation 4(b) of the POPIA Regulations, specifically for any deployment of wearable technology that captures biometric or health data.

Looking Ahead

South Africa has both the constitutional foundation and the legislative architecture through POPIA to shape the regulatory response to wearable AI across the continent. The Information Regulator has not yet issued specific guidance on smart wearables, but the trajectory is unmistakable: the

draft Code of Conduct on controlled-entry-point data collection, the compliance monitoring programme, and the Regulator's enforcement action against WhatsApp for applying weaker privacy terms to South African users than to Europeans^[13] all signal a regulator that will not tolerate a two-tier approach to data protection.

Specific AI legislation is not imminent in 2026, but POPIA already provides a comprehensive framework for regulating wearable AI.

Are these devices already in your building? The question is whether your compliance framework has kept pace.

[1] Apple Newsroom 'Introducing AirPods Pro 3, the ultimate audio experience' <https://www.apple.com/newsroom/2025/09/introducing-airpods-pro-3-the-ultimate-audio-experience/> (accessed 09-09-2026).

[2] PetaPixel 'Meta Smart Glasses Face Calls for Bans Across Europe Over Privacy Concerns' <https://petapixel.com/2026/08/04/meta-smart-glasses-face-calls-for-bans-across-europe-over-privacy-concerns/> (accessed 09-09-2026). France's CNIL issued its warning on 11 May 2026.

[3] 5thscape Blog 'Meta Smart Glasses Privacy Test Expands to Germany' <https://5thscape.com/blog/meta-smart-glasses-germany-privacy/> (accessed 09-09-2026).

[4] ALM Corp 'Meta Ray-Ban AI Smart Glasses: UK Investigation & US Lawsuit' <https://almcorp.com/blog/meta-ray-ban-ai-smart-glasses-privacy-investigation-uk-us/> (accessed 09-09-2026).

[5] *Bartone v Meta Platforms Inc* Case 3:26-cv-01897 (ND Cal, filed March 2026).

[6] A Juma 'How smart glasses are rewriting the rules of consent in South Africa' <https://www.intelligentio.com/africa/2026/05/26/how-smart-glasses-are-rewriting-the-rules-of-consent-in-south-africa/> (accessed 09-09-2026).

[7] Apple Support 'Track your heart rate during workouts with AirPods Pro 3' <https://support.apple.com/guide/airpods/track-heart-rate-workouts-airpods-pro-3-dev1b40fb47d/web> (accessed 09-09-2026).

[8] The study was presented at CHI 2026 by researchers at Tsinghua University and the University of Utah, concluding that notification mechanisms in camera glasses 'prove inadequate' as bystander safeguards. See TechTimes 'Germany Invokes Cayla Spy-Device Law Against Meta Smart Glasses' <https://www.techtimes.com/articles/324064/20260812/germany-invokes-cayla-spy-device-law-against-meta-smart-glasses-owners-face-destruction-risk.htm> (accessed 09-09-2026).

[9] The Verge 'Meta tightens privacy policy around Ray-Ban glasses to boost AI training' <https://www.theverge.com/news/658602/meta-ray-ban-privacy-policy-ai-training-voice-recordings> (accessed 09-09-2026).

[10] Popular Mechanics 'Meta's Smart Glasses Have Even Bigger Privacy Issues Than We Thought' <https://www.popularmechanics.com/technology/gear/a70782916/meta-smart-glasses-privacy-report-spring-2026/> (accessed 09-09-2026). See also ALM Corp (note 5 above).

[11] EU Perspectives 'Meta smart glasses: MEPs question regulator on privacy protection' <https://euperspectives.eu/2026/03/meta-smart-glasses-meps-question-regulator-on-privacy-protection/> (accessed 09-09-2026).

[12] A Burger-Smidt 'Information Regulator signals tougher POPIA and PAIA enforcement' <https://www.moonstone.co.za/information-regulator-signals-tougher-popia-and-paia-enforcement/> (accessed 09-09-2026).

[13] Information Regulator Enforcement Notice against WhatsApp (16 April 2025).



Ahmore Burger-Smidt

Head of Regulatory

[View Profile](#)