WERKSMANS
ATTORNEYS

DATA PRIVACY | REGULATORY

When the clock starts ticking..... Why cross-border data breach response demands more than good intentions

9 September 2026 *7 min read*

by Ahmore Burger-Smidt, Director and Head of Regulatory, and Tebogo Sibidla, Director

Picture this.

A retailer with operations spanning southern and eastern Africa discovers on a Friday evening that a threat actor has exfiltrated customer records from a compromised cloud environment. The breach touches individuals in Kenya, Zambia, Zimbabwe, and South Africa. In Zambia and Zimbabwe, the clock gives them just 24 hours to notify the regulator.[1] In Kenya, they have 72 hours, unless their systems qualify as critical information infrastructure, in which case the window shrinks to a mere 24 hours.[2] South Africa's POPIA, by contrast, imposes no fixed-hour deadline at all, requiring notification only "as soon as reasonably possible".[3]

And the regulatory bodies receiving those notifications? Entirely different institutions, with different forms, different portals, and different expectations.

Welcome to the reality of cross-border breach response in 2026.

The Myth of the Universal Playbook

Too many organisations still treat data breach response as a single procedure, a single plan, a single template, a single timeline. That approach was always fragile. Today, it is genuinely dangerous.

Across sub-Saharan Africa alone, the legislative landscape has shifted dramatically in the past three years. Botswana replaced its 2018 Act with substantially enhanced breach-notification obligations in 2024, introducing a 72-hour reporting window and prison terms of up to nine years for certain violations. Malawi's Data Protection Act came into force in June 2024, with its own 72-hour reporting requirement and a novel public notification mechanism via newspapers when direct notice requires disproportionate effort or expense. Tanzania enacted comprehensive data protection legislation in 2022, backed by administrative fines up to TZS 100 million and criminal imprisonment of up to ten years. These are not legacy frameworks gathering dust, they are recent, actively enforced, and strikingly divergent from one another.

The Devil Lives in the Differences

What makes cross-border compliance genuinely difficult is not the existence of notification obligations, most sophisticated organisations expect those. The difficulty lies in the granular inconsistencies.

Firstly, timelines pull in different directions. Rwanda requires notification to the NCSA within 48 hours. Nigeria mirrors the GDPR's 72-hour notification standard for the NDPC. Uganda requires notification "immediately" upon discovery. Ghana offers no fixed hour count at all, relying instead on a "reasonably practicable" standard. When a single incident spans four of these jurisdictions, the compliance team must operationalise the shortest deadline as the effective floor, while still satisfying the specific procedural requirements of each.

Secondly, notification thresholds diverge significantly. South Africa and several other countries require reporting of all security compromises irrespective of assessed risk level. Kenya and Nigeria, echoing GDPR principles, trigger individual notification only where there is a "*likely high risk*" to rights and freedoms. Botswana requires reporting unless the breach is unlikely to result in a risk to the rights and freedoms of the data subject. Morocco doesn't impose a mandatory notification regime at all, merely a strong expectation of responsible incident management from the CNDP.[4] For a single breach affecting data subjects across these territories, the compliance team faces a zero-threshold obligation, divergent risk-based obligations, and a soft-law expectation simultaneously.

Thirdly, the level of detail required in data breach notifications differs significantly across jurisdictions. At one end of the spectrum, Zambia does not prescribe what must be included in a notification. Ghana adopts a general standard, requiring only "sufficient information" to allow the data subject to take protective measures. Botswana, Kenya, Malawi and Nigeria prescribe detailed content requirements closely aligned with the GDPR. South Africa goes further, requiring additional elements including the identity of the intruder (if known). Kenya imposes more onerous requirements: a chronological account of steps taken, details of how the breach occurred, and prescribed document uploads including the incident response policy, internal incident logs, and copies of reports sent to other regulators.

Fourthly, penalties vary widely. Kenya's administrative fines cap at KES 5 million or 1% of annual turnover.[5] Rwanda imposes fines of RWF 2–5 million or 1% of prior-year global turnover.[6] Botswana has adopted what observers describe as a "GDPR-plus enforcement posture," with potential prison terms of up to nine years.[7] Criminal sanctions, including imprisonment, feature across Nigeria, Tanzania, and Uganda.[8]

Building a Jurisdiction-Aware Response Framework

So, what does good practice look like? A few principles stand out.

1. Map your exposure before the breach happens. In-house teams should maintain a living matrix that documents the notification obligations, timelines, thresholds, and designated authorities for every jurisdiction in which they process personal data. This is not a once-off exercise, but must be reviewed and updated whenever there are legislative or other developments in a country's data protection regulatory framework. Botswana, Malawi, and Tanzania all overhauled their frameworks within the past two years.[9]
2. Design for the tightest deadline. If your operations affect Zambia or Zimbabwe, your internal escalation and triage processes must be able to produce a regulatory notification within 24 hours. That becomes the design constraint for your entire incident response architecture.
3. Appoint jurisdiction leads, not a single breach coordinator. Each relevant jurisdiction requires someone who understands the local regulator's expectations, prescribed forms, portal requirements, and the practical nuances of engagement.
4. Invest in threshold analysis upfront. Because jurisdictions apply different tests, from South Africa's all-in approach to Kenya's risk-based trigger, a rapid, defensible methodology for assessing severity across multiple frameworks is essential. You cannot afford to work this out on the night of discovery.

The Direction of Travel

The trajectory is unmistakable. Namibia remains the conspicuous outlier, lacking a comprehensive data protection statute, but political pressure following the 2025 NSFAF data breach has intensified calls to finalise its draft Bill.[10] Elsewhere, the pattern is one of convergence toward mandatory, time-bound notification regimes, with increasingly severe penalties for non-compliance.

For organisations operating across multiple African jurisdictions and, indeed, globally, the message is straightforward. The window for treating breach response as a reactive, ad hoc exercise has closed. What is needed now is infrastructure: legal mapping, operational readiness, jurisdictional expertise, and the institutional muscle to execute across borders under intense time pressure.

The breach will come.

The only question is whether your response architecture was built for the world as it actually is, fragmented, fast-moving, and unforgiving of those who failed to prepare.

---

[1] Data Protection Act 3 of 2021 (Zambia) s 24; Cyber and Data Protection Act [Chapter 12:07] of 2021 (Zimbabwe) s 29.

[2] Data Protection Act 24 of 2019 (Kenya) s 43. The Data Protection (General) Regulations, 2021 (Kenya) prescribe a 72-hour notification period, reduced to 24 hours for operators of designated critical information infrastructure.

[3] Protection of Personal Information Act 4 of 2013 (POPIA) s 22(1). From April 2025, the Information Regulator introduced a mandatory e-Services Portal for reporting security compromises.

[4] Law No 09-08 of 18 February 2009 on the Protection of Individuals with regard to the Processing of Personal Data (Morocco), with implementing Decree 2-09-165. No general GDPR-style mandatory breach notification regime with fixed timelines exists; the Commission Nationale de contrôle de la protection des Données à caractère Personnel (CNDP) expects "prompt and responsible incident management."

[5] Data Protection Act 24 of 2019 (Kenya) s 62. Administrative fines up to KES 5 million or 1% of annual turnover (whichever is lower) for controllers; KES 3 million or 0.5% of turnover for processors.

[6] Law No 058/2021 (Rwanda) art 68. Administrative fines of RWF 2–5 million or 1% of prior-year global turnover for misconducts including failure to notify or report a breach.

[7] Data Protection Act 18 of 2024 (Botswana). Described as among the strictest breach-related penalty regimes in the region, adopting a notably GDPR-plus enforcement posture.

[8] Nigeria Data Protection Act, 2023 (n 8 above) s 48 (up to one year's imprisonment for non-compliance with NDPC orders); Personal Data Protection Act 11 of 2022 (Tanzania) s 62 (criminal fines and imprisonment up to 10 years); Data Protection and Privacy Act 9 of 2019 (Uganda) ss 39–40 (administrative penalties and compliance orders).

[9] Data Protection Act 18 of 2024 (Botswana); Data Protection Act 3 of 2024 (Malawi); Personal Data Protection Act 11 of 2022.

[10] Draft Data Protection Bill, 2021 (Namibia). No comprehensive data protection statute is currently in force; only the constitutional right to privacy under article 13 of the Constitution of the Republic of Namibia, 1990 applies.

Ahmore Burger-Smidt

Head of Regulatory

View Profile

Tebogo Sibidla

Director

View Profile