



Regulatory Alert

Consent, legitimate interest, and the line between them

What Rwanda's Data Protection Law means for event organisers, schools, churches, and every business that handles personal data





It started at a concert in Kigali...

Picture this. It's a Saturday night at an open-air music festival in Kigali. You dance, the official photographer captures the moment and disappears into the crowd.

The next morning, your face is plastered across social media as the headline image for a completely different commercial event. You ask the organiser to take it down. The reply? "You bought a ticket and entered the venue. Our terms say that counts as consent to use your image."

So here's the question every Rwandan should be asking: **does buying a ticket mean you've given away your right to privacy?** The answer is a resounding **no**.

Rwanda's **Law N° 058/2021 of 13/10/2021 relating to the Protection of Personal Data and Privacy** was enacted to protect you, your photos, your videos, your personal information from exactly this kind of thing. The law is overseen by the **NCSA—Data Protection Office of Rwanda**, the national authority responsible for enforcing your data protection rights. And as Kigali positions itself as a hub for world-class concerts, conferences, and international events, those rights matter more than ever.

This alert is your guide. Let's walk through what "consent" really means told through the stories of people who could be your neighbours.

Did you know? Under Rwandan law, unlawful processing of sensitive personal data such as religious beliefs captured on a church livestream can carry up to **ten years' imprisonment** and fines of **RWF 25,000,000**. Even for ordinary personal data, corporate bodies face fines of up to **5% of annual turnover**. And these rules are already being enforced across East Africa.

Meet Muhire, Uwimana, and Uwase

To understand what your rights look like in real life, let's follow three people through situations you might recognise. Their stories move from the dance floor, to the pew, to the classroom but the thread running through all of them is the same: what does it really mean to give your consent?

Muhire's story: "I bought a ticket—not a modelling contract"

Muhire bought a ticket to a major festival in Kigali and danced all night. A week later, his photo appeared on posters advertising for a different paid event. He never agreed to that. When Muhire complained, the organiser pointed to a line buried deep in the ticketing terms and conditions: "By entering the venue, you consent to the use of your image for promotional purposes."

It sounds convincing but the law says otherwise. Muhire's experience raises the central legal question at the heart of this alert: **what does valid consent actually require?** The answer lies in four requirements. Under **Article 3(18)** of Rwanda's Data Protection Law, consent must be **freely given, specific, informed, and unambiguous** demonstrated through a clear statement or deliberate action. These four pillars will reappear in every story that follows. Let's test the organiser's defence against each one:

- **Freely given** — Muhire must have a genuine choice to say yes or no, with no strings attached. Under **Article 6**, consent is invalid if it is a condition for accessing a service like buying a ticket. The rationale is straightforward: if saying "no" means losing something you are entitled to, the "choice" is coerced, not free. This also means consent is compromised where there is a **power imbalance** such as between an employer and an employee, or a public authority and a citizen because the freedom to truly refuse is structurally absent.
- **Specific** — A "yes" to attending a concert is not a "yes" to commercial marketing. Blanket consent, a single broad checkbox covering multiple unrelated purposes, is not legally valid. The law requires that each distinct purpose of data processing be consented to separately, so that the data subject knows exactly what they are agreeing to and can accept one purpose while refusing another.
- **Informed** — Before you agree, you must be told: who is collecting your data, why, what categories of data are being collected, whether it will be shared with third parties or transferred across borders, how long it will be retained, and your right to withdraw consent at any time. These transparency requirements are set out under **Article 42** of the law. The principle is that consent given in ignorance of material facts is not meaningful consent; the data subject must have enough information to make a genuine decision.
- **Unambiguous** — Silence, pre-ticked boxes, or simply walking through a gate do not count. Even posing for a photograph does not automatically mean you have agreed for it to be used in commercial promotions. There must be a clear, deliberate action and an affirmative step that leaves no reasonable doubt about the data subject's intention. The law places the burden on the data controller to demonstrate that such an action occurred.

On every count, the organiser's defence fails. But this isn't just theory: **regulators in East Africa have already ruled on cases just like Muhire's**. While these cases come from Kenya, they carry weight across the region: East African data protection frameworks share common principles, and Rwandan regulators and courts are likely to find this emerging body of enforcement decisions persuasive as they develop their own jurisprudence.

In *Antonate Rombo Aiko v. Goodtimes Africa T/A Blankets & Wine* (Kenya ODPC, Complaint No. 2175 of 2025), a woman discovered her photograph was being used to promote a future paid event by the organisers of Blankets & Wine. The organiser argued that consent was covered by the general T&Cs shared with ticket buyers. The Data Protection Commissioner flatly rejected this, ruling that general terms **cannot** cover commercial marketing and ordered the organiser to pay KES 300,000 (approximately USD 2,500) in direct damages. In another case (*Perpetual Wanjiku v. Casa Vera Lounge*), the Commissioner ruled that unilateral entry disclaimers and posing for a photographer are legally insufficient to justify publishing images for commercial marketing on social media.

The penalties under Rwandan law are no joke. Under **Article 56**, the unlawful collection and use of personal data is an offence punishable by imprisonment of one to three years, a fine of RWF 7 million to RWF 10 million, or both. Corporate offenders may additionally face fines of up to 5% of annual turnover under Article 62. To put that in perspective: for a mid-sized company, that's enough to build several homes.

Muhire's story established the foundation: the four-part consent test under Article 3(18), and the reality that a buried clause in the fine print satisfies none of its requirements. But there is an important legal distinction the next story will test. Muhire's data was a photograph, what the law treats as ordinary personal data. When data reveals something more intimate like religious belief it crosses into a separate legal category called **sensitive personal data**, and the consequences of mishandling it are far more severe.

Uwimana's story: "The Church livestreamed my prayer — Did anyone ask me first?"

Uwimana attends a local congregation in Kigali every Sunday. One Sunday, the church livestreamed the entire service on Facebook. A close-up of Uwimana, mid-prayer and in tears, was broadcast to thousands. She only found out when a colleague mentioned it at work on Monday.

The church meant well. **But good intentions don't change the law** and Uwimana's story raises a distinct legal question: **what happens when the data being captured is sensitive?**

The law creates a two-tier system. Muhire's photograph was ordinary personal data. Uwimana's situation is legally different: filming someone in deep worship and broadcasting it online reveals their religious beliefs. Under Article 3 of Rwanda's Data Protection Law, religious beliefs and biometric data are classified as sensitive personal data. This classification is not merely a label; it triggers an entirely separate penalty regime.

For ordinary personal data, the consequences of non-compliance are criminal: under Article 56, unlawful processing carries imprisonment of one to three years and fines of RWF 7,000,000 to RWF 10,000,000, or both. Corporate offenders face fines of up to 5% of annual turnover under Article 62 as in Muhire's case. For sensitive personal data, the consequences become criminal. Under Article 60, the unlawful collection or processing of sensitive personal data carries 7 to 10 years of imprisonment and fines of RWF 20,000,000 to RWF 25,000,000. The jump is significant: from a maximum fine of RWF 10,000,000 and imprisonment of one to three years under Article 56, to a maximum fine of RWF 25,000,000 and imprisonment of seven to ten years under Article 60. This escalation is a deliberate policy choice; the law recognises that certain categories of data carry a higher risk of harm to the individual if misused and calibrates the penalty accordingly.

The trend extends beyond East Africa. South Africa's Information Regulator under POPIA has issued strict reminders that religious organisations are **not exempt** from data protection laws and cannot capture or broadcast congregant media without explicit consent. The direction of enforcement across the continent is clear.

So the next time your church sets up a camera, ask yourself: did they ask for my permission?

Uwimana's story tested the second tier of the law: **sensitive personal data**. The four-part consent test still applies, but failure now triggers criminal penalties imprisonment, not just fines. The next story tests a third and final legal layer: what happens when the data subject lacks the legal capacity to consent at all? Under Rwandan law, children under 16 cannot give consent themselves and that changes who bears the obligation entirely.

Uwase's story: "My child's face is on the school's TikTok — Now what?"

Uwase's sister sends her a TikTok video from her daughter's school children at a sports day, with the school's logo overlaid. A marketing video. Nobody asked Uwase for permission. The school's response? "We sent a message on the parents' WhatsApp group. And you paid your school fees that cover it."

It doesn't. And Uwase's story introduces the law's most protective layer: **what happens when the data subject cannot consent at all?**

Muhire's case tested whether consent was freely given. Uwimana's tested whether sensitive data was handled lawfully. Uwase's goes further because children **cannot legally consent for themselves**, and the law places the obligation squarely on parents and guardians.

Under **Article 9** of Rwanda's Data Protection Law, processing a child's personal data (for any child under 16) is lawful **only** if consent is given or authorised by the holder of **parental responsibility**. This is not a softer standard it is the same four-part test from Article 3(18) that failed the event organiser in Muhire's story, applied with an additional gatekeeper requirement. A WhatsApp message is not a clear affirmative action. Payment of school fees is not specific to data processing. Neither is informed, and neither is freely given.

The penalties reflect how seriously the law treats violations involving children: Under **Article 56**, unlawfully collecting, using, sharing, or disclosing personal data is punishable by **one to three years of imprisonment** and fines of **RWF 7,000,000 to RWF 10,000,000**. Note that Article 56 applies to the act of unlawful processing itself where the data involved is also sensitive (as children's data often is), Article 60's heavier penalties may apply in parallel.

A Kenyan case proves this isn't theoretical. In *Christine Wairimu Muturi v. Roma School Uthiru*, a parent lodged a complaint alleging that the school was posting images and videos of minors on TikTok and Facebook for marketing without parental consent. The school argued that a WhatsApp group notification and the payment of fees constituted consent. The Data Commissioner rejected this entirely, ruling that a WhatsApp notification does not satisfy the requirement for affirmative, informed consent for processing children's data. The school was found liable for multiple violations of children's rights.

Parents and guardians, you are the gatekeepers of your children's data. If no one asked you properly, the law says it shouldn't have happened.

Uwase's story tested the law's final and most protective layer: **parental consent as a gatekeeper** for children's data. Together, the three stories trace a deliberate structure in the law the same four-part consent test under Article 3(18) applies throughout, but the severity of consequences escalates with the vulnerability of the data subject: administrative fines for ordinary personal data, criminal imprisonment for sensitive data, and compounding penalties where children are involved.

The following table summarises the penalty escalation across the three stories:

Story	Data Type	Key Articles	Maximum Fine	Imprisonment
Muhire	Ordinary personal data	Arts. 56 and 62	RWF 10,000,000 (individuals) / 5% of annual turnover (corporate bodies)	1–3 years
Uwimana	Sensitive personal data	Art. 60	RWF 25,000,000	7–10 years
Uwase	Children's personal data	Arts. 9, 56 and 60	RWF 10,000,000 (Art. 56) / RWF 25,000,000 (Art. 60)	1–3 years (Art. 56) / 7–10 years (Art. 60)

But wait — What about public events like car free days?

If you've been reading carefully, you might be asking: "What about when the government photographs people at a car free day and posts the images on social media? Thousands of Rwandans participate, their faces are visible, and nobody signs a consent form. Is that a violation too?"

It's an important question and the answer reveals a crucial nuance in the law that every reader should understand.

Consent is not the only lawful basis for processing personal data. The three stories above Muhire, Uwimana, and Uwase all involve situations where the organisation **claimed consent** as its legal basis and failed to meet the four-part test. But Rwanda's Law N° 058/2021 also recognises other lawful grounds for processing, including **public interest, legitimate interest, legal obligation, and contractual necessity**. When a government body photographs a public health initiative like a car free day and shares the images to promote civic participation, it is not relying on your individual consent it may be relying on **public interest or public task** basis—not your individual consent.

This changes the legal analysis entirely. The question is no longer "did they get my consent?" but rather "did they have a lawful basis, and was their use proportionate?"

Global courts and regulators have grappled with exactly this distinction. In Canada, the Supreme Court in *Aubry v. Éditions Vice-Versa* (1998) held that publishing an identifiable photograph of a person taken in a public place, without consent, for commercial purposes violated the individual's image rights but acknowledged exceptions for matters of **public interest and information purposes**. In the European Union, the GDPR recognises both **legitimate interest** (Article 6(1)(f)) and **public task** (Article 6(1)(e)) as lawful bases, and European regulators have generally accepted that photographing crowds at public events where individuals are not the primary subject can be lawful when the purpose is governmental, journalistic, or informational. The UK's Information Commissioner's Office has issued guidance noting that people at public outdoor events generally have a **lower expectation of privacy** than those in private spaces, though this does not extinguish their rights entirely.

So where does the line fall? Based on global practice, it typically comes down to these factors:

Factor	Generally lawful without consent	Potentially problematic
Subject	Crowd or atmosphere shot	Identifiable individual singled out
Purpose	Public information, government communications	Commercial marketing or advertising
Controller	Government body or media	Private commercial entity
Setting	Open public space	Ticketed or semi-private venue
Data type	Ordinary data (face in a crowd)	Sensitive data revealed (religion, health)
Proportionality	Image proportionate to the stated purpose	Excessive, unrelated, or repurposed use

Applied to a car free day: a government body photographing crowds participating in a public health initiative, in an open public space, for the purpose of promoting that initiative, is in a fundamentally different legal position from an event organiser who buries a likeness waiver in the fine print and uses your close-up to sell tickets to a different show.

But the protection doesn't disappear entirely. Even in public spaces, if a government body singles out a specific, identifiable individual say, using a close-up of one person as the lead image of an unrelated campaign the proportionality question sharpens. And if the image reveals sensitive personal data (for example, religious attire, a visible disability, or political affiliation), the heightened protections under Article 60 may apply regardless of the setting.

What about private companies? Consent vs. legitimate interest

The car free day example involves a government body acting in the public interest. But what about a **private company** say, a hotel chain that photographs its grand opening, a telecom sponsor that captures images at a marathon, or a restaurant that posts photos of diners on Instagram?

Private companies cannot rely on the **public task** basis that is reserved for public authorities. But they may, in some circumstances, rely on **legitimate interest** as an alternative to consent. Under most data protection frameworks, including Rwanda's Law N° 058/2021, legitimate interest requires the company to demonstrate three things:

- **A genuine, lawful interest** — for example, promoting the company's services or documenting a corporate event.
- **Necessity** — the processing must be necessary to achieve that interest, and there must not be a less intrusive way to accomplish the same goal.
- **A balancing test** — the company's interest must not be overridden by the **rights and freedoms** of the individuals whose data is being processed. This is where most claims fail.

The balancing test is critical. A hotel posting a wide-angle shot of a busy lobby to showcase its atmosphere may pass. A hotel singling out an identifiable guest and using their close-up as a Facebook advertisement likely does not because the individual's reasonable expectation was to eat dinner, not to become a marketing asset.

The Kenyan cases in this alert illustrate exactly this failure. In both *Aiko v. Blankets and Wine* and *Wanjiku v. Casa Vera Lounge*, the organisations were private commercial entities that used identifiable images of individuals for commercial promotion. Whether framed as consent or legitimate interest, the outcome would likely be the same: the individual's rights outweigh the company's marketing interest when the person has been singled out, was not informed, and had no opportunity to object.

The practical lesson for private companies: legitimate interest is not a loophole around consent. It is a separate legal basis with its own rigorous requirements. If your primary purpose is commercial marketing using identifiable images, consent remains the safest and most defensible path. Legitimate interest is better suited for incidental, crowd-level, or operational processing where singling out individuals is not the purpose.

The takeaway for readers is this: **the alert's three stories address the most common and most problematic scenario—where organisations claim consent but don't actually have it.** That remains the core risk for most Rwandans in their daily lives. But the broader legal framework is more nuanced: governments may rely on public interest, and private companies may in limited circumstances rely on legitimate interest. Not every photograph taken at every public event is a violation. Context, purpose, and proportionality matter.

Where to raise a complaint

If your data has been used without valid consent, you have the right to take action. The **NCSA—Data Protection Office of Rwanda** is the national authority responsible for enforcing the Law relating to the Protection of Personal Data and Privacy. If you believe your rights have been violated whether by an event organiser, a place of worship, a school, or any other organisation you can lodge a complaint with the NCSA.

Your consent checklist: The path forward is privacy by design

The stories of Muhire, Uwimana, and Uwase aren't hypothetical, they are built on real complaints that regulators across East Africa have already ruled on. The pattern is consistent: hidden terms fail. Passive notices fail. Assumptions that attendance equals consent fail. The path forward is **Privacy by Design** building genuine, informed consent into every process from the start, not as an afterthought. Even though Rwanda has not yet developed a substantial body of court decisions on data protection, the legal obligations already exist. Consent is a **legal duty**, not something triggered only by litigation.

This checklist is your starting point.

For individuals — Protect yourself:

- **Read before you tick.** Don't accept blanket terms and conditions without checking what you're actually consenting to.
- **Ask the right questions.** Who is collecting my data? Why? For how long? Will it be shared?
- Know that silence is not consent. Walking into a venue, attending a service, or paying school fees does not equal permission.
- **Remember you can say no**—and you can withdraw consent at any time.
- **Speak up.** If your image or data is used without proper consent, the law is on your side.
- **Parents: be the gatekeeper.** Ask your child's school for their data protection policy on children's images. If they don't have one, demand one.
- **Share this alert.** Tell your family, friends, and neighbours about their rights.

For organisations — Get compliant:

- **Audit your consent practices.** Are you relying on blanket T&Cs, entry disclaimers, or WhatsApp notifications? These are not valid consent.
- **Implement separate, specific consent forms** for each distinct use of personal data (e.g. event photography, marketing, data sharing with sponsors).
- **Provide full transparency** before asking for consent: who you are, what data you're collecting, why, who you'll share it with, and how long you'll keep it.
- **Make consent genuinely voluntary.** Never tie access to a service or benefit to a consent requirement.
- **Appoint and empower a Data Protection Officer (DPO)** to oversee compliance.
- **Train your staff.** Everyone who handles personal data must understand the rules.
- **Pay special attention to sensitive data** (religious beliefs, biometrics) and children's data the penalties for getting these wrong are the most severe.
- **Document everything.** Be able to demonstrate that valid consent was obtained if a regulator comes knocking.

Want to go deeper?

This alert was prepared by the **Data Protection and Privacy Team at PwC Rwanda**, specialists in data governance, regulatory compliance, and privacy advisory across East Africa. PwC is hosting a related training session: **Inside the Breach: The Data Protection Playbook from East Africa's landmark cases** on Friday, 9 October 2026 at Ubumwe Grand Hotel, Kigali from 8am–4:30pm. The **NCSA — Data Protection Office of Rwanda** will be in attendance.

[Click here to register for the training](#), or contact PwC Rwanda.

This alert is published by PwC for general information purposes only and does not constitute legal advice. Readers should seek independent professional advice on the specific facts and circumstances of their situation before taking any action based on the content of this alert. PwC accepts no liability for any loss arising from any action taken or not taken in reliance on this publication.



Paul Frobisher Mugambwa

Head of Tax, Legal and Fiscal Policy Leader at PwC Rwanda
frobisher.mugambwa@pwc.com
+250 782 537 377



Herbert Njoroge

Senior Manager in Legal Business Solutions at PwC Kenya
herbert.njoroge@pwc.com
+254 746 108 655



Doreen Uwamahoro

Trainee Associate in Tax and Legal Business Solutions at PwC Rwanda
doreen.uwamahoro@pwc.com
+250 796 897 832





At PwC, we help clients build trust and reinvent so they can turn complexity into competitive advantage. We're a tech-forward, people-empowered network with more than 364,000 people in 136 countries and 137 territories. Across audit and assurance, tax and legal, deals and consulting, we help clients build, accelerate, and sustain momentum. Find out more at www.pwc.com. PwC refers to the PwC network and/or one or more of its member firms, each of which is a separate legal entity. Please see www.pwc.com/structure for further details. © 2026 PwC. All rights reserved (2026-467-76)