# Why data protection in Rwanda goes beyond registration

June 2026

## You got the Certificate. Now What?

Let us give credit where it is due. Since Rwanda passed its data protection law (Law N° 058/2021 of 13/10/2021 relating to the Protection of Personal Data and Privacy), there has been a real surge in organisations registering as data controllers and processors with the **Rwanda Data Protection and Privacy Office under the National Cyber Security Authority (DPO–NCSA)**. The law is clear: if you want to handle people's personal data, you must register. Think of it as your licence to operate. And to be fair, most organisations have done exactly that. Bravo.

**But here is the uncomfortable truth—and forgive the bluntness—a certificate on your wall does not mean the data in your systems is safe**. Registration is like getting a driving licence. It proves you passed the test, but it does not mean you are actually driving safely every day. Too many organisations in Rwanda have collected their certificate, dusted off their hands, and declared themselves "compliant." Meanwhile, the real work of data protection with its many rules, responsibilities, and potential pitfalls—remains largely untouched. The glaring gap? Organisations stop at registration and never bother to implement the full set of legal requirements that come with being a data controller or processor. Registration is the starting line, not the finish line. And the uncomfortable reality is this: many organisations in Rwanda today are compliant on paper but exposed in practice.

## Registration: Getting your foot in the door

Now, to be fair, registration is not just a matter of filling in a form and pressing submit. Under the law, you have to tell the DPO–NCSA quite a lot: who you are, what personal data you will process, why you are processing it, who you will share it with (and for how long), whether it will leave the country, and what risks are involved (plus how you plan to manage them). If everything checks out, you get your certificate within thirty working days.

But that certificate comes with strings attached. If anything changes about how you handle data, you must report it to the DPO–NCSA within fifteen working days. If your certificate is about to expire, you need to apply for renewal at least forty-five working days before it runs out. And if you gave false, misleading, or even incomplete information, or if you stop following the rules? The DPO–NCSA can cancel your certificate entirely. Ouch.

So yes, registration matters—it is your legal foundation. But if your entire compliance strategy relies on a certificate hanging on the wall, you have a problem. A potentially very costly one.

# Cross-border data transfers: Where most organisations fall short

This is where things get interesting—and where many organisations get it spectacularly wrong. The law is crystal clear: you cannot send any personal data outside Rwanda unless you have:

- obtained specific authorisation from DPO–NCSA after proving you have proper safeguards in place, and
- obtained the data subject's consent.

Let us pause and think about what "sending data outside Rwanda" actually looks like in the real world. You are a company with offices across Africa or beyond. Every morning, your employees log into Workday—a platform whose servers are definitely not in Kigali. Your teams chat on Microsoft Teams, sharing documents and client information that bounces through servers scattered across the globe. Your HR records sit on cloud infrastructure that colleagues in Johannesburg or London can access with a few clicks. Emails, SharePoint files, internal databases—all of these are invisible highways carrying personal data across borders every single day. And most organisations do not even realise it is happening.

So here is the million-dollar question: how many of these organisations have actually obtained the required authorisation from the Data Protection and Privacy Office? The answer, one suspects, would make for very uncomfortable reading.

Now here is what makes this even more serious: the authorisation you get is incredibly specific. It names exactly who you can send data to and for what purposes. The conditions are strict and non-negotiable: the data must be anonymised before transfer; you cannot transfer any data that was not specified in your application; you cannot transfer data for any purpose you did not declare; you cannot send it to any country you did not list; and you cannot disclose it to anyone you did not name. Re-identifying data that has been de-identified is also expressly prohibited.

Let that sink in. This authorisation is not a blanket passport for your data to roam freely wherever your corporate network reaches. It is laser-specific to the recipients, purposes, and countries you declared. So, if you told the DPO–NCSA you are transferring HR data to your Nairobi office via Workday, that does not automatically cover the fact that your finance team in London can also access the same system. Each organisation must ensure its application captures the full picture—every flow, every platform, every destination—both domestically between branches and internationally across borders.

To make matters more complex, the transfer authorisation does not exist in a vacuum. It is issued subject to other regulators' rules too—particularly those relating to outsourcing regulations. So your data protection obligations can overlap with sector-specific rules, adding extra layers of accountability. Think of it as a compliance sandwich: data protection law on top, sector regulation in the middle, and your internal policies at the bottom. Every layer has to hold.

There is one more thing: if you authorise someone outside Rwanda to access or receive personal data, you must sign a written contract with them. This contract must spell out who does what, who is responsible for what, and how both parties will comply with the law. Transfer is not just a technical exercise—it is a legal commitment that must be documented and enforceable.

## The elephant in the server room: Where is your data actually stored?

If the transfer authorisation is the rule organisations overlook, the hosting certification is the one they pretend does not exist. The law sets a powerful default: personal data must be stored in Rwanda. Period. You can only store it outside Rwanda if you hold a specific certificate from the DPO–NCSA allowing you to do so.

Now consider the reality of how businesses actually operate today. Your HR system runs on Workday. Your emails live on Microsoft's cloud. Your financial data sits on Oracle's servers. Your documents are on Google's platform. Where, exactly, is all that personal data being stored? Almost certainly not in Rwanda. And if you do not have the right authorisation for that, you have a problem.

The hosting authorisation is platform-specific—it names the exact platforms you are allowed to use for storing data (for example, Workday, Microsoft, Oracle, or Google). You must ensure the data is properly protected and inform the Data Protection and Privacy Office if anything changes.

This specificity is not bureaucratic box-ticking—it is the law. If you start using a new cloud platform, switch providers, or even upgrade to a service tier that routes data through different countries, you must notify the DPO–NCSA and potentially apply for a new or amended authorisation. You cannot just assume your existing certificate covers whatever new technology you adopt next.

The bottom line: if you are storing personal data on any platform outside Rwanda without the DPO–NCSA's express, platform-specific permission, you are breaking the law. Full stop.

## What is happening across Africa—and why it should wake you up

Rwanda does not exist in a bubble, and the rest of the continent is not standing still. Across Africa, the data protection landscape is evolving fast—and it should make any organisation still treating registration as the finish line very, very nervous. Regulators, courts, and civil society groups are increasingly holding organisations accountable not just for whether they registered, but for what they did (or failed to do) afterwards. The logic is simple: if you cannot even handle the basic step of registration properly, why should anyone trust you with the harder stuff—cross-border transfers, hosting, breach notifications, or impact assessments?

Here are some recent developments from around the continent that carry direct lessons for Rwanda (you can read more in **The East African Privacy Monthly · Issue 2 – May 2026):**

**Kenya. When a telecom giant gets caught.** Kenya's High Court recently delivered a landmark ruling against one of the country's biggest telecoms. The company was found to have violated subscribers' constitutional rights to privacy and dignity after a massive breach involving the unauthorised extraction and sharing of subscriber data. The Court said data controllers bear direct constitutional obligations; you cannot hide behind the excuse of "rogue employees" when your systems and governance are fundamentally broken. Damages were awarded to affected subscribers. The lesson for Rwanda? Registration alone does not protect you. Without proper technical and organisational safeguards (the kind required under Article 47 of Rwanda's Law), you are exposed no matter how many certificates you hold. If a major telecom in Kenya can be found wanting, organisations in Rwanda operating without transfer or hosting authorisations are playing with fire.

**Uganda. People are going to prison for this.** A court in Kampala convicted three mobile money agents for unlawfully obtaining and disclosing a client's personal data—and they had also failed to register with the data protection authority. This was only the second criminal conviction under Uganda's framework. Read that again: people are being criminally convicted—not just fined—for data protection violations. In Rwanda, the law prescribes imprisonment of up to 3 years and fines of up to Frw 10 million (USD 6,800) for unlawful transfers. If you are moving data across borders without authorisation, you are not just "non-compliant" in some abstract regulatory sense. You could be committing a criminal offence.

**Uganda. Health data sharing put under the spotlight.** Privacy professionals publicly criticised a health data sharing agreement between Uganda and the United States, pointing out that it lacked a data protection impact assessment, had no adequacy determination, and completely excluded the data protection authority from the framework. The takeaway for Rwanda? Cross-border data sharing whether through government agreements or your company's internal systems demands proper safeguards. Having a data sharing agreement is not enough; that agreement must actually comply with the law. And if your staff are sharing data through Teams or SharePoint across borders, that counts as a cross-border transfer whether you realise it or not.

**Nigeria. African regulators are teaming up**. Nigeria recently hosted data protection authorities from nine African countries to drive cross-border regulatory cooperation and harmonise privacy frameworks. Regulators from across the continent, plus regional bodies like ECOWAS, CEMAC, and IGAD, gathered specifically to strengthen enforcement and enable seamless data flows. The signal is clear: what may seem like a purely domestic Rwandan issue today could become the subject of cross-border regulatory scrutiny tomorrow. If you operate in multiple African countries, you cannot afford to be compliant in one and negligent in another.

**Tanzania. The grace period is over.** Tanzania's data protection law is now in full enforcement, and its regulator has announced a first-ever Annual Data Privacy Conference. Like Rwanda, Tanzania's framework is new but it is moving rapidly from paper to practice. Across the region, the days of "we are still getting ready" are ending. Regulators expect action, not excuses.

**Kenya. Data protection is now a profession.** The Data Privacy and Governance Society of Kenya has grown to over 900 members and has been actively involved in litigation, policy dialogue, and cross-border collaboration. Data protection is no longer a side task that you give to your IT department or legal intern, it is a full professional discipline. In Rwanda, organisations need to start building real internal capacity: appointing data protection officers, training staff, and engaging with the regulatory community.

The pattern across the continent is unmistakable. Regulators are moving beyond registration towards real enforcement. Courts are handing out real penalties including prison sentences. Cross-border data flows are under the microscope. Organisations that treat compliance as a tick-box exercise, register and carry on as normal are finding themselves on the wrong side of courts, regulators, and public opinion. **If all you have done is register, you have barely scratched the surface.** Rwanda's organisations would be wise to take note and to act now, not later.

## The penalties: What happens if you get this wrong

Let's talk money and freedom. If you access, collect, use, share, transfer, or disclose personal data in a way that breaks the law, you are looking at imprisonment of one to three years, and fines between Frw 7 million and Frw 10 million (USD 4,700 to USD 6,800). **Or both. And for companies? A fine of 5% of your entire annual turnover from the previous financial year. 5% of global turnover. Let that number sink in.**

Even lesser violations like operating without a valid certificate or letting it expire attract fines of Frw 2 million to Frw 5 million (USD 1,400 to USD 3,400), or 1% of global turnover. And the DPO–NCSA has a nuclear option: it can prohibit or suspend the transfer of personal data outside Rwanda altogether. It can also demand that any controller or processor prove their compliance at any time. No warning required.

For a large multinational whose entire business model depends on data flowing seamlessly across borders, having that flow suspended would be nothing short of catastrophic. Imagine waking up one morning and being told your global systems cannot touch Rwandan personal data until further notice. Operations grind to a halt. Clients lose confidence. Revenue evaporates. This is not a theoretical risk—it is a very real possibility for anyone ignoring these rules.

> The math is simple: compliance is always cheaper than consequences. Always has been, always will be.

## So what should you actually do? A practical roadmap

Rwanda has made an impressive start in putting data protection on the national agenda, backed by clear legislation and growing institutional muscle. The grace period for voluntary compliance is over, full compliance is now expected. Regulators want to see real, comprehensive data protection practices, not just a registration certificate.

If your organisation transfers personal data in any way to affiliated offices abroad, to global service providers, to partners, or simply through internal systems accessible from other countries, you typically need not one, but three distinct certifications:

- Registration as a data controller or processor
- Authorisation to transfer personal data outside Rwanda
- Authorisation to host personal data on platforms outside Rwanda

Each is specific to your declared purposes, recipients, countries, and platforms. They're not interchangeable, and they are definitely not optional.

One more critical point: these certifications are specific to you. You cannot assume that because another organisation got authorised to use a particular platform or transfer route, the same applies to your organisation. Your application must reflect your specific data flows, your specific platforms, and your specific recipients. Precision matters. Accuracy matters. In data protection, compliance is quite literally personal.

The era of treating registration as the sum total of compliance is decisively over. The organisations that will thrive in Rwanda's regulatory landscape are those that invest in understanding and obtaining the full suite of certifications, maintain them diligently, and report changes promptly. Those that do not? They will find themselves explaining to regulators, courts, and clients why they thought the front door was the entire building.

# How PwC can help you get this right

Feeling overwhelmed? That is completely understandable and exactly why we are here. PwC can help you figure out exactly which certifications you need and guide you through the entire process from start to finish. Here is what we offer:

- **Registration as a data controller or processor.** We help you prepare and submit your registration application, making sure all the required details what data you process, why, who sees it, where it goes, and how you manage risks are captured accurately. We also keep you on track with ongoing obligations like reporting changes, renewing on time, and staying within the terms of your certificate.
- **Authorisation for transferring data outside Rwanda.** We map all your cross-border data flows including the ones you might not have thought about, like data moving through Workday, Teams, SharePoint, and Outlook, and prepare comprehensive applications for transfer authorisation. We make sure every recipient, purpose, country, and transfer method is properly identified, and that you understand the strict conditions attached (including anonymisation requirements and the prohibition on going beyond what your application says). We also help draft the written contracts required between you and anyone receiving data outside the country.
- **Authorisation for hosting data outside Rwanda.** We help you identify every platform and service provider storing your personal data outside Rwanda and apply for the hosting authorisation you need. This includes making sure each platform is specifically named, advising you on notification obligations when things change, and helping with amendments or fresh applications when you adopt new technology.
- **Full-spectrum data protection advisory.** Beyond the three core certifications, we provide end-to-end advisory covering everything the law requires: appointing data protection officers, conducting impact assessments, setting up breach notification procedures, maintaining processing records, and implementing proper security measures. We help you build a compliance framework that is proactive rather than reactive, one where data protection is woven into your daily operations, not treated as a one-off project.
- **Customised training that actually sticks.** We design and deliver tailored training programmes for your organisation from board-level awareness sessions to hands-on operational training for teams that handle personal data every day. Our programmes are customised to your sector, size, and risk profile because effective compliance requires more than policies on paper. It requires people who understand what those policies mean in practice.
- **Policy review and compliance document development.** We review your entire policy bundle privacy notices, consent frameworks, data retention policies, breach response plans, access request procedures, and data sharing agreements identifying gaps and drafting what needs fixing. We also develop the key compliance documents most organisations need but do not have: data protection impact assessments, data flow maps, records of processing activities, breach notification templates, consent forms, and cross-border transfer agreements. These are the documents that prove compliance in practice, not just in principle.
- **Bespoke frameworks for unique organisations.** We specialise in helping organisations with unique structures, NGOs, international development bodies, and civil society organisations build data protection frameworks tailored to their specific realities. These organisations often handle highly sensitive data about vulnerable populations across multiple countries and through complex partnerships. We design governance structures and operational procedures that embed data protection into the organisation's DNA, ensuring compliance is sustainable, proportionate, and genuinely fit for purpose, not a generic template borrowed from a different sector.

# Contacts


## Paul Frobisher Mugambwa

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



## Ineza Uwase Nancy

Associate in Tax and Legal Business Solutions at PwC Rwanda
nancy.ineza@pwc.com
+250 787 501 156



www.pwc.com